Fano's Geometry and Hamming Code

Michael Eby, Taylor Stevens, Godwin Atuahene

Department of Mathematics, Baldwin Wallace University Berea, Ohio 44017

Project Mentor: Dr. Brent Strunk

Introduction

Finite geometries explore the connections of points, lines, and planes rather than their shape. A finite geometry is a collection of points and lines defined by a set of incidence axioms, defining their existence and connection, and often a parallel axiom. In the case of projective geometries like Fano's, the negation of the parallel axiom is assumed, so each pair of lines intersects at a point.

Finite geometry has numerous applications in networking and computer science. In this presentation, we explore one application to the Hamming code, a type of error-correction coding widely used for transmitting data over noisy networks and for preserving the integrity of data in memory or storage for essential applications. We focus here in particular on Fano's geometry, also called the seven point geometry or PG(2,2).

Real World Application

Hamming coding is a method of adding redundant information to a message so that if an error occurs in transmission, it can be detected and corrected at the receiving end. Hamming coding relies on techniques from linear algebra that can be discovered through the use of finite geometries. In the (7,4) Hamming code, the message is broken into 4-bit chunks, and each chunk has 3 error-correction bits added by means of left-multiplying by a generator matrix G. The columns of G can be determined by using the Fano plane as a model. The person receiving the transmission then breaks it into 7-bit chunks and checks for errors by left-multiplying by the parity-check matrix H. If the result is the zero vector, no errors have occurred, and the first four bits of that chunk are the correct message. If the result is any other vector, the bit with the number of the column corresponding to the resultant vector was flipped during transmission. Note that this method can only detect and correct a single bit error in the 7-bit codeword. If more than one error occurs, they will not be corrected.

The only challenge is to generate the correct matrices G and H so that if w is the intended 4-bit message, Gw will be a 7-bit codeword, and HGw will be a 3-bit zero vector, while if x differs from w only in its nth bit, HGx will be the nth column of G. These matrices can be derived from the Fano Plane coordinatized by the field $F_2^3 = \{0,1\}^3$.

Concept

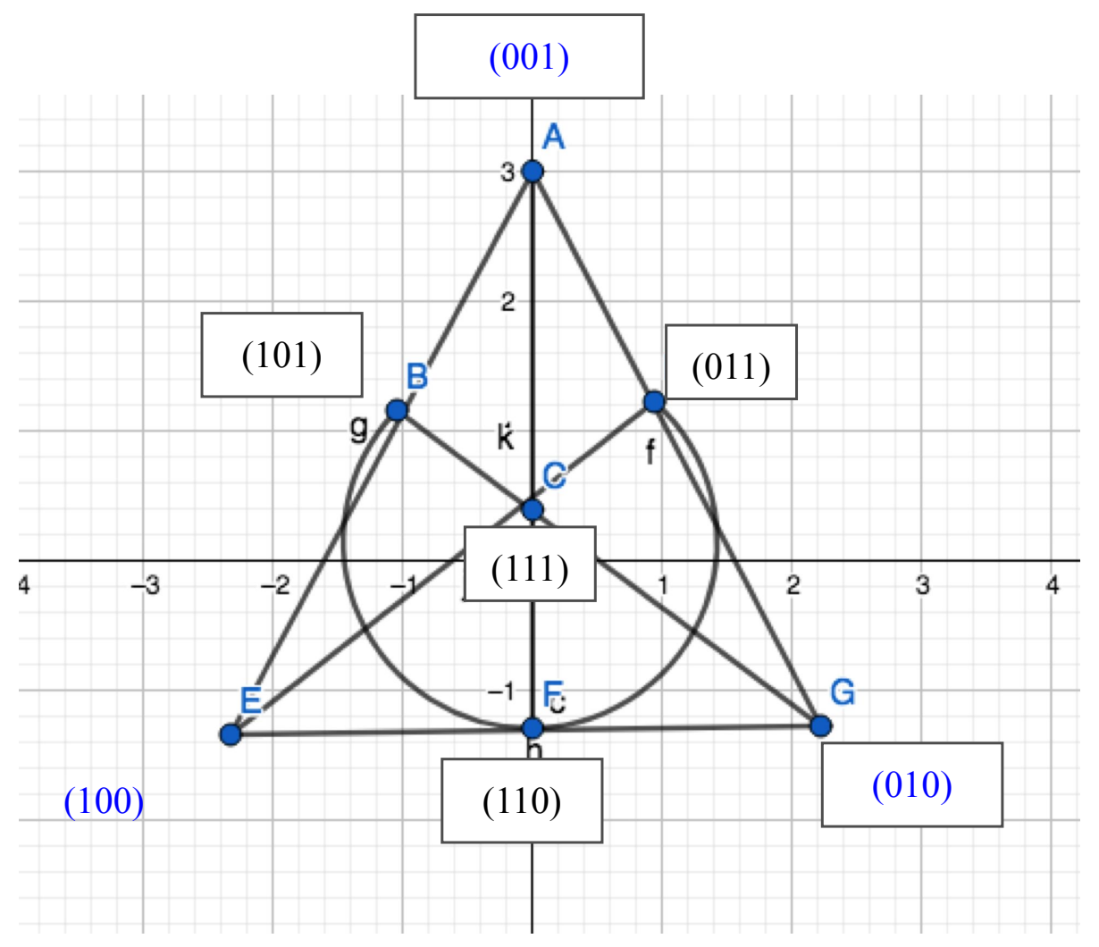

Figure 1. Fano's Geometry with coordinates.

To generate G and H from the Fano plane, we first assign each point three coordinates, with the rule that the sum (mod 2) of any two points on any line equals the third point on that line. This relies on the essential properties of the Fano plane: that it has 7 points and 7 lines, with 3 points on each line.

There is just one way up to symmetry to coordinatize the plane with F_2^3 that follows this rule. The coordinates of these points will give us the codewords for our (7,4) Hamming code and the matrices G and H. The coordinates of the seven points make up the seven columns of H, where three of them form the identity matrix as the last three columns and the other four are in any order. Calling this H = [P I], where I is the identity matrix, we get $G = \begin{bmatrix} I \\ -P \end{bmatrix} = \begin{bmatrix} I \\ P \end{bmatrix}$ (where the second equality is only true here because 1 = -1 (mod 2) and 0 = -0). The blue columns in H below correspond to the blue coordinates of points of the Fano plan above.

$$H = \begin{array}{c} \begin{array}{cc} \mathrm{P} & \mathrm{I} \end{array} \\ \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \end{array}, \quad G = \begin{array}{c} \mathrm{I} \\ \\ \\ \\ \mathrm{P} \\ \\ \end{array} \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{array}\right]$$

With the matrices generated, the code is easy to use. For instance, if I want to send the message "0100111001001111" (UTF-8 for "NO") to Godwin, I would first break it into 4-bit chunks "0100," "1110," "0100," and "1111." Call these w_1, w_2, w_3, and w_4, respectively. I then compute $Gw_1 = c_1$, $Gw_2 = c_2$, $Gw_3 = c_3$, and $Gw_4 = c_4$. I concatenate the codewords to get the bit string $c_1c_2c_3c_4$ and send the transmission through a noisy channel. $Gw_1 = c_1 = [0100101]^T$, but suppose the first bit flipped from 0 to 1 due to interference, so Godwin receives $[1100101]^T$. He then computes Hc_1, Hc_2, Hc_3, and Hc_4. Hopefully they should each give the zero vector, but in this case, $H[1100101]^T = [011]^T$, which is the first column of H. This means the first bit of c_1 was flipped during transmission. Godwin can flip it back, then concatenate the first four bits of each c to retrieve the original message.

The Elevator Pitch

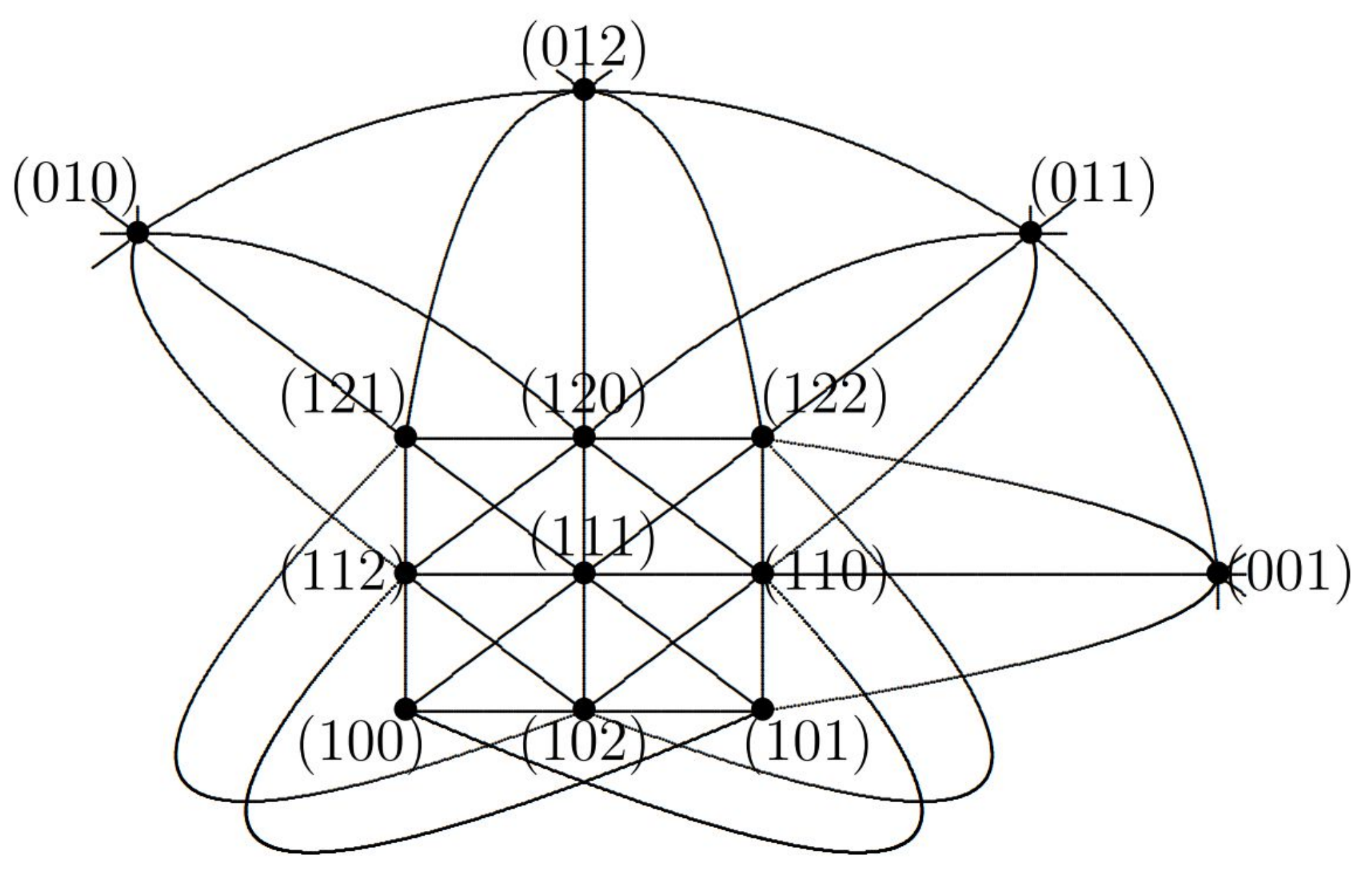

Figure 2. PG(3,2) with coordinates in F_3^3. (Fleming 09)

Geometric models are useful in other branches of math because they allow us to apply theorems of geometry. For instance, the Cartesian plane allows us to leverage our theorems and intuitions about areas and tangency to calculus. In this example, we were able to apply ideas about collinearity in a geometric sense to linear dependence in algebra.

Most importantly, we can generalize the (7,4) Hamming code by using larger projective geometries than the Fano plane. The diagram above is the geometry PG(3,2) with 13 points and lines. Because it has the same essential properties as the Fano plane, it will generate codewords for an error-correcting code in the same way. In general, it is a theorem that for every positive integer q, there is a projective geometry of order q with q^2+q+1 points and lines. This gives us an infinite family of Hamming codes of different sizes and an intuitive explanation for why the (7,4) Hamming code uses 7 bits per codeword.

Alternatively, we can generate larger error-correcting codes besides Hamming code by moving to higher dimensions. For instance, PG(3,3), a 3-dimensional projective geometry, can be used to generate error-correcting codes in the same manner. However, working with higher dimensions often causes the geometries to contain coordinates that are not binary and this makes these geometries less useful when working with computers.

Formal Proof

Fano's geometry
undefined terms: *point*, *line*, and *on*
Axiom 1. There exists at least one line.
Axiom 2. There are exactly three points on every line.
Axiom 3. Not all points are on the same line
Axiom 4. There is exactly one line on any two distinct points.
Axiom 5. There is at least one point on any two distinct lines.

Fano's geometry has exactly 7 points and exactly 7 lines.

Pf: Suppose Fano's Geometry.
By A1, we have L1 and by A2 it has the points a, b, c.
By A3, we have the point d that is not on L1.
By A4, we have L2, $\overline{ad}$, L3, $\overline{bd}$, and L4, $\overline{cd}$.
By A2, we have the points e, f, g with e on L2, f on L3, and g on L4.
By A4, we have the lines L5, $\overline{efc}$, and L6, $\overline{gfa}$.
By A4, L7 must connect $\overline{eg}$.
By A5, L7 must intersect L1, L2, … , L6.
  L7 intersects L2, L4, L5, L6
  So L7 must intersect L1 and L3.
  So by A2 the 3rd point on L7 must be b.
(Proving there are exactly 7 lines)
If there was a line L8, by A5 it must intersect the other 7 lines.
Without loss of generality, choose a.
If L8 is on a, L8 intersects L1, L2, and L6.
By A5 it must intersect L3, L4, and L5.
For L8 to intersect L3 it must contain the points b, f, or d.
By A4, if L8 contains the points b, f, or d, it is the same line as L1, L2, or L6.
So L8 is not unique. So no L8.

Literature cited

Flemin, Patrick. 2009. "Error Correcting Codes and Finite Projective Planes." Presented to the Mathematics and Computer Science Department, South Dakota School of Mines and Technology. April 16 & 17. https://micsymposium.org/mics_2009_proceedings mics2009_submission_52.pdf

Pell, Timothy. 2005. Applications of Finite Geometry. <http://web.mnstate.edu/peil/geometry/C1AxiomSystem/4summary.htm> Accessed on 2019 Nov 12.

Wallace, E.C. and S.F West. 2015. *Roads to Geometry. 3rd* ed. Long grove, IL: Waveland Press.

Acknowledgments

A special thanks to Fano for being a G.

For further information

Please contact Michael Eby at eebstersc@gmail.com, Taylor Stevens at tstevens16@bw.edu, or Godwin Atuahene at gatuahen19@bw.edu. A digital version of this poster is available at https://docs.google.com/presentation/d/e/2PACX-1vRsLXZPqj6GkUZkLznjYxiQ9SVI8CKAY4zom_uVTHH9eeD6FbbeeOjorywCWEO3TGSiI5iHk75CWE51/pub.