ALETHEIA
The Alpha Chi Journal of Undergraduate Scholarship

Volume 7 | Issue 2 | 2022

Spheres in $\mathbb{F}_q^3$

Benjamin Norton and
Jeremy Chapman, PhD

Lyon College
Arkansas Iota Chapter

Vol. 7(2), 2022
Article Title: Spheres in $\mathbb{F}_q^3$
DOI:10.21081/ax0344
ISSN:2381-800X
Key Words: Finite fields, spheres.

Author contact information is available from tlindblom@alphachihonor.org or kvosevich@alphachihonor.org.

Volume 7 | Issue 2 | 2022

Article Title: Spheres in $\mathbb{F}_q^3$
DOI: 10.21081/ax0344
ISSN: 2381-800X

ALETHEIA
The Alpha Chi Journal of Undergraduate Scholarship

Spheres in $\mathbb{F}_q^3$

Benjamin Norton and Jeremy Chapman, PhD

Lyon College
Arkansas Iota Chapter

Abstract

Euclid's *The Elements* shows that a unique circle in $\mathbb{R}^2$ is determined by three noncollinear points. In [4] it is shown that circles can be similarly determined in $\mathbb{F}_q^2$, the two-dimensional vector space over the finite field $\mathbb{F}_q$. More specifically, it is shown that three noncollinear points which have nonzero distance from each other determine a unique circle of nonzero radius. In this paper, we extend this result to show that four noncoplanar points in $\mathbb{F}_q^3$ determine a unique sphere. However, unlike the two-dimensional case, ensuring the four points are nonzero distance from each other does not guarantee that the sphere will have a nonzero radius.
Keywords: Finite fields, spheres

1 Introduction

We would like for any undergraduate student with a reasonable mathematics background to be able to read this paper. Therefore, as in [4], we provide the following basic information which allows us to define a finite field. See [3] to find more information about groups, rings, and fields, see [5] for more details regarding vectors spaces and matrix theory, and see [8] to find out more about lines and planes in $\mathbb{R}^3$.

Before getting into the definitions, we should mention that a similar result to Theorem 1.15 is proven in [7]. However, in this paper we go further by using zero lines to show that choosing the four noncoplanar points to be nonzero distance from each other is not sufficient to obtain a nonzero radius sphere. Although the technique of our proof is similar, we provide significantly more background, detail, and justification. Specifically, we prove that the coefficient matrix of the system has a nonzero determinant and find an explicit formula for the center of the sphere. We begin with the following definition of a group.

Definition 1.1. The set G defines a *group* with respect to the binary operation $*$ if the following are satisfied:

1. G is closed under $*$.
2. $*$ is associative.
3. G has an identity element, e.
4. Every element of G has an inverse. For each $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$.

Note that if $*$ on G is commutative, then G is called an *abelian group*.

Definition 1.2. The set R defines a *ring* with respect to addition and multiplication if the following are satisfied:

1. R forms an abelian group with respect to addition.
2. R is closed with respect to an associative multiplication.
3. The following two distributive laws hold: $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$.

In the case that multiplication in R is commutative, then R is called a *commutative ring*.

Definition 1.3. The set F defines a *field* if the following are satisfied:

1. F is a commutative ring.
2. F has a unity $1 \neq 0$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in F$.
3. Every nonzero element of F has a multiplicative inverse.

Every field is an integral domain, meaning that there are no zero divisors [3]. Zero divisors are nonzero elements of a ring which can be multiplied by another nonzero element to yield zero.

Definition 1.4. A field that has a finite number of elements is called a *finite field*.

It is known that the order of every finite field is the power of a prime [6]. In this paper, we use $\mathbb{F}_q$ to denote a finite field with q elements where $q = p^l$, $p > 2$ is a prime, and $l \in \mathbb{N}$. Note that since $\mathbb{F}_q$ is a finite integral domain, the characteristic of the unity 1 is p [3]. In other words, p is the least positive integer such that $p \cdot 1 = 0$. Since $p > 2$ it follows that $2 \neq 0$.

Throughout this paper, we will use the following notation:

1. $\frac{a}{b}$ will represent $(a)(b^{-1})$, where b^{-1} is the multiplicative inverse of b.

2. $a-b$ will represent $a+(-b)$, where $-b$ is the additive inverse of b.

Definition 1.5. Let $\mathbb{F}$ be a field. A *vector space* is a set V along with an addition on V and a scalar multiplication on V such that the following properties hold (see [1]):

1. $u + v = v + u$ for all $u, v \in V$.

2. $(u + v) + w = u + (v + w)$ and $(ab)v = a(bv)$ for all $u, v, w \in V$ and all $a, b \in \mathbb{F}$.

3. There exists an element $0 \in V$ such that $v + 0 = v$ for all $v \in V$.

4. For every $v \in V$, there exists $w \in V$ such that $v + w = 0$.

5. $1v = v$ for all $v \in V$.

6. $a(u + v) = au + av$ and $(a + b)u = au + bu$ for all $a, b \in \mathbb{F}$ and all $u, v \in V$.

In this paper we work exclusively in $\mathbb{F}_q^3$, the three-dimensional vector space over the finite field $\mathbb{F}_q$. Just as $\mathbb{R}^3$ is the set of all ordered triples of real numbers, one can think of $\mathbb{F}_q^3$ as all ordered triples of elements of $\mathbb{F}_q$, that is, $\mathbb{F}_q^3 = \{(x, y, z) : x, y, z \in \mathbb{F}_q\}$.

Definition 1.6. The *norm*, or distance, between two points $P_1 = (x_1, y_1, z_1)$ and $P_2 = (x_2, y_2, z_2)$ where P_1, $P_2 \in \mathbb{F}_q^3$, denoted $||P_2 - P_1||$, is $(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2$.

Note that in vector spaces over finite fields, it is possible for two distinct points to possess zero distance.

Example 1.7. Consider $\mathbb{Z}_7^3$, the three-dimensional vector space over the finite field $\mathbb{Z}_7$. We use bar notation to denote the congruence classes, that is, $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. In this particular field, modular arithmetic allows us to demonstrate zero distance between the points $(\overline{5}, \overline{6}, \overline{4})$ and $(\overline{2}, \overline{1}, \overline{3})$. Substituting these points into the norm equation, we get $||P_2 - P_1|| = (\overline{5} - \overline{2})^2 + (\overline{6} - \overline{1})^2 + (\overline{4} - \overline{3})^2 = \overline{9} + \overline{25} + \overline{1} = \overline{35} = \overline{0}$, since $35 \equiv 0 \pmod 7$.

Definition 1.8. As in $\mathbb{R}^3$, a *line* in $\mathbb{F}_q^3$ is determined by a point on the line and the direction of the line. We define the line through (x_0, y_0, z_0) parallel to $\langle a, b, c\rangle$ to be the set of points $\{(x_0 + at, y_0 + bt, z_0 + ct) : t \in \mathbb{F}_q\}$.

Definition 1.9. A *zero line* is a line where each point on the line is zero distance from all of the other points on the line. See [4] for more details.

Definition 1.10. A *plane* in $\mathbb{F}_q^3$ is represented by a point (x_0, y_0, z_0) on the plane and a vector $\vec{n} = \langle a, b, c\rangle$ that is normal to the plane, where $a, b, c \in \mathbb{F}_q$. We can then write the scalar equation of the plane as $a(x-x_0)+b(y-y_0)+c(z - z_0) = 0$ or equivalently $ax + by + cz + d = 0$ where $d = -ax_0 - by_0 - cz_0$.

Before getting into the linear algebra needed to prove our main result, it is worth mentioning that although introductory linear algebra courses usually use $\mathbb{R}$ or $\mathbb{C}$ as the base field, essentially every result is independent of the base field. In other words, we can use $\mathbb{F}_q$ as the base field in place of $\mathbb{R}$ or $\mathbb{C}$. In the next section we demonstrate how standard linear algebra techniques such as Gauss-Jordan elimination still work in this setting.

Definition 1.11. Let $M_{n\times n}(\mathbb{F}_q)$ be the set of matrices of size $n \times n$ whose entries belong to $\mathbb{F}_q$. The $n \times n$ *identity matrix*, I_n, is a matrix consisting of 1's along the main diagonal and 0's elsewhere. The *inverse* of a matrix $A \in M_{n\times n}(\mathbb{F}_q)$, denoted A^{-1}, is a matrix that satisfies the equation $AA^{-1} = A^{-1}A = I_n$. Such a matrix A is also said to be *invertible*.

Definition 1.12. For $n \geq 2$, the *determinant* of $A \in M_{n\times n}(\mathbb{F}_q)$, denoted either as $\det(A)$ or $|A|$, is given by the equation $\det(A) = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij})$, where a_{ij} is the element in the ith row and jth column of matrix A, and A_{ij} is the submatrix obtained by deleting the ith row and the jth column of A. In particular, the 2×2 determinant $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$. A 3×3 determinant will be calculated later as an exercise.

Theorem 1.13 (Invertible Matrix Theorem)**.** *If $A \in M_{n\times n}(\mathbb{F}_q)$, then the following statements are equivalent:*

1. *A is an invertible matrix.*

2. *The equation $A\vec{x} = \vec{b}$ has a unique solution for every $n \times 1$ column matrix $\vec{b}$.*

3. *The equation $A\vec{x} = \vec{0}$ has only the trivial solution where $\vec{0}$ is the $n \times 1$ zero matrix.*

4. *The determinant of A is not equal to zero.*

See [5] for a statement and proof of Theorem 1.13 in its entirety; for brevity we only list the conditions that will be utilized within the proof of Theorem 1.15.

Definition 1.14. A *sphere* in $\mathbb{F}_q^3$ is defined as the set of all points equidistant from its center. In particular, a sphere centered at C of radius r is given by $S_r(C) = \{P \in \mathbb{F}_q^3 : ||C-P|| = r\}$.

Figure 1 depicts a sphere of radius three over $\mathbb{Z}_7^3$ to provide an example of what such a sphere would look like.

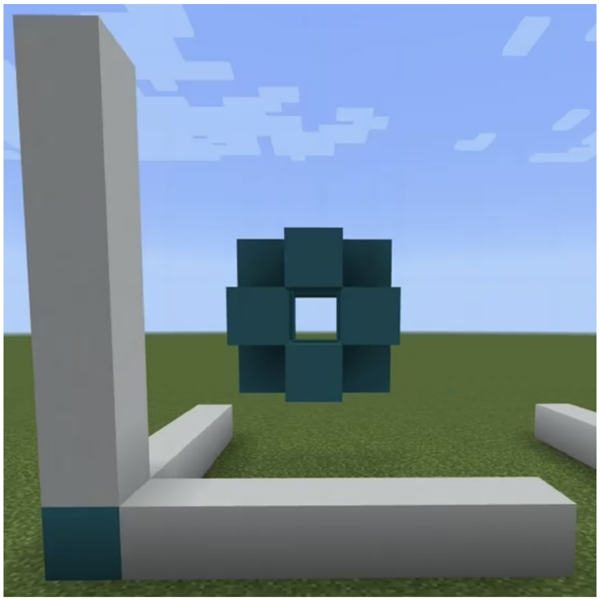

Figure 1: A sphere of radius three centered at $(\overline{3},\overline{3},\overline{3})$ over $\mathbb{Z}_7^3$. The origin $(\overline{0},\overline{0},\overline{0})$ is not included the sphere, the point is colored in this instance merely to indicate its position for orientation purposes. Screenshot taken from the video game *Minecraft*.

Our main result is the following.

Theorem 1.15. *If $P_1, P_2, P_3, P_4 \in \mathbb{F}_q^3$ are four distinct, noncoplanar points, then they determine a unique sphere in $\mathbb{F}_q^3$.*

2 Exhibition of Linear Algebra Techniques

As a demonstration that linear algebraic techniques continue to be applicable when the base field is a finite field, we provide an example of Gauss-Jordan elimination finding the inverse of a matrix. In the subsequent example, we find the determinant of a 3×3 matrix using cofactor expansion.

Note 2.1. It is sufficient to use $\mathbb{Z}_p$ in place of $\mathbb{F}_p$ as $\mathbb{Z}_p$ and $\mathbb{F}_p$ are isomorphic. See [6] for a proof of this fact.

Example 2.2. Let $A \in M_{2\times 2}(\mathbb{Z}_7)$, $A = \begin{bmatrix}\overline{1} & \overline{3}\\ \overline{1} & \overline{2}\end{bmatrix}$ where $\begin{vmatrix}\overline{1} & \overline{3}\\ \overline{1} & \overline{2}\end{vmatrix} = \overline{1}\cdot\overline{2} - \overline{3}\cdot\overline{1} = \overline{6} \neq \overline{0}$. Since the determinant is nonzero, by Theorem 1.13 we know there exists an inverse A^{-1}. To find the inverse using Gauss-Jordan elimination, augment matrix A with I_2 and row reduce:

$$\left[\begin{array}{cc|cc}\overline{1} & \overline{3} & \overline{1} & \overline{0}\\ \overline{1} & \overline{2} & \overline{0} & \overline{1}\end{array}\right] \xrightarrow{-R_1+R_2\to R_2} \left[\begin{array}{cc|cc}\overline{1} & \overline{3} & \overline{1} & \overline{0}\\ \overline{0} & \overline{6} & \overline{6} & \overline{1}\end{array}\right]$$
$$\xrightarrow{\overline{6}R_2\to R_2} \left[\begin{array}{cc|cc}\overline{1} & \overline{3} & \overline{1} & \overline{0}\\ \overline{0} & \overline{1} & \overline{1} & \overline{6}\end{array}\right] \xrightarrow{-\overline{3}R_2+R_1\to R_1} \left[\begin{array}{cc|cc}\overline{1} & \overline{0} & \overline{5} & \overline{3}\\ \overline{0} & \overline{1} & \overline{1} & \overline{6}\end{array}\right]$$

This gives $A^{-1} = \begin{bmatrix}\overline{5} & \overline{3}\\ \overline{1} & \overline{6}\end{bmatrix}$, which can be verified by checking $AA^{-1} = \begin{bmatrix}\overline{1} & \overline{3}\\ \overline{1} & \overline{2}\end{bmatrix}\cdot\begin{bmatrix}\overline{5} & \overline{3}\\ \overline{1} & \overline{6}\end{bmatrix} = \begin{bmatrix}\overline{1} & \overline{0}\\ \overline{0} & \overline{1}\end{bmatrix} = I_2$.

Example 2.3. To find the determinant of a 3×3 matrix, multiply each entry of a row or column by its respective cofactor matrix as follows:

$$\begin{aligned}\det(A) &= \begin{vmatrix}a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{vmatrix}\\ &= a_1\begin{vmatrix}b_2 & c_2\\ b_3 & c_3\end{vmatrix} - a_2\begin{vmatrix}b_1 & c_1\\ b_3 & c_3\end{vmatrix} + a_3\begin{vmatrix}b_1 & c_1\\ b_2 & c_2\end{vmatrix}\\ &= a_1(b_2c_3 - b_3c_2) - a_2(b_1c_3 - b_3c_1) + a_3(b_1c_2 - b_2c_1)\\ &= a_1b_2c_3 - a_1b_3c_2 - a_2b_1c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1.\end{aligned}$$

In particular, for $A = \begin{bmatrix}\overline{1} & \overline{3} & \overline{4}\\ \overline{2} & \overline{3} & \overline{1}\\ \overline{3} & \overline{3} & \overline{1}\end{bmatrix} \in M_{3\times 3}(\mathbb{Z}_5)$, we can use the equation above to find the following determinant:

$$\begin{aligned}\det(A) =& (\overline{1}\cdot\overline{3}\cdot\overline{1}) - (\overline{1}\cdot\overline{3}\cdot\overline{1}) - (\overline{2}\cdot\overline{3}\cdot\overline{1})\\ &+ (\overline{2}\cdot\overline{3}\cdot\overline{4}) + (\overline{3}\cdot\overline{3}\cdot\overline{1}) - (\overline{3}\cdot\overline{3}\cdot\overline{4})\\ =& \overline{3} - \overline{3} - \overline{1} + \overline{4} + \overline{4} - \overline{1}\\ =& \overline{1}\end{aligned}$$

Note 2.4. Let $A = \begin{bmatrix}a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{bmatrix}$. One application of determinants is the following theorem found in [5] in which the inverse of a matrix can be found by the following equation:

$$A^{-1} = \frac{1}{\det(A)}\,\mathrm{adj}(A)$$

where $\mathrm{adj}(A)$ is the transpose of the cofactor matrix, which is found by replacing each $a_{ij} \in A$ with $\det(A_{ij})$. By Theorem 1.13 we know that if A is invertible, then $\det(A) \neq 0$, so $\frac{1}{\det(A)}$ is in fact defined. We can then find the inverse as follows:

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$$
$$= \frac{1}{\det(A)} \begin{bmatrix} +\begin{vmatrix} b_2 & c_2 \\ b_3 & c_3 \end{vmatrix} & -\begin{vmatrix} a_2 & c_2 \\ a_3 & c_3 \end{vmatrix} & +\begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} \\ -\begin{vmatrix} b_1 & c_1 \\ b_3 & c_3 \end{vmatrix} & +\begin{vmatrix} a_1 & c_1 \\ a_3 & c_3 \end{vmatrix} & -\begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \\ +\begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix} & -\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} & +\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \end{bmatrix}^T$$
$$= \frac{1}{\det(A)} \begin{bmatrix} +(b_2c_3 - b_3c_2) & -(a_2c_3 - a_3c_2) & +(a_2b_3 - a_3b_2) \\ -(b_1c_3 - b_3c_1) & +(a_1c_3 - a_3c_1) & -(a_1b_3 - a_3b_1) \\ +(b_1c_2 - b_2c_1) & -(a_1c_2 - a_2c_1) & +(a_1b_2 - a_2b_1) \end{bmatrix}^T$$
$$= \frac{1}{\det(A)} \begin{bmatrix} (b_2c_3 - b_3c_2) & (a_3c_2 - a_2c_3) & (a_2b_3 - a_3b_2) \\ (b_3c_1 - b_1c_3) & (a_1c_3 - a_3c_1) & (a_3b_1 - a_1b_3) \\ (b_1c_2 - b_2c_1) & (a_2c_1 - a_1c_2) & (a_1b_2 - a_2b_1) \end{bmatrix}^T$$
$$= \frac{1}{\det(A)} \begin{bmatrix} (b_2c_3 - b_3c_2) & (b_3c_1 - b_1c_3) & (b_1c_2 - b_2c_1) \\ (a_3c_2 - a_2c_3) & (a_1c_3 - a_3c_1) & (a_2c_1 - a_1c_2) \\ (a_2b_3 - a_3b_2) & (a_3b_1 - a_1b_3) & (a_1b_2 - a_2b_1) \end{bmatrix}$$

Exercise 2.1. Gauss-Jordan elimination can be used to find the inverse of any invertible $n \times n$ matrix. As an exercise, use both methods to find A^{-1} where $A = \begin{bmatrix} \overline{9} & \overline{4} & \overline{2} \\ \overline{2} & \overline{5} & \overline{6} \\ \overline{1} & \overline{3} & \overline{4} \end{bmatrix}$ is an element of $M_{3\times3}(\mathbb{Z}_{11})$. Verify that your answer is correct by checking that $A \cdot A^{-1} = I_3$.

3 Proof of Theorem 1.15

Let $P_1, P_2, P_3, P_4 \in \mathbb{F}_q^3$ be four noncoplanar points. Say $P_1 = (x_1, y_1, z_1), P_2 = (x_2, y_2, z_2), P_3 = (x_3, y_3, z_3)$, and $P_4 = (x_4, y_4, z_4)$. As in [4], if P_1, P_2, P_3, and P_4 all lie on the same sphere with center $C = (x, y, z)$, then the distance from P_1 to C must be the same as the distance from P_2 to C and so on, which yields the following equations.

$$\begin{aligned} &||P_1 - C|| = ||P_2 - C|| \\ \implies &(x_1 - x)^2 + (y_1 - y)^2 + (z_1 - z)^2 = (x_2 - x)^2 + (y_2 - y)^2 + (z_2 - z)^2 \\ \implies &x_1^2 - 2xx_1 + x^2 + y_1^2 - 2yy_1 + y^2 + z_1^2 - 2zz_1 + z^2 = x_2^2 - 2xx_2 + x^2 + \\ &y_2^2 - 2yy_2 + y^2 + z_2^2 - 2zz_2 + z^2 \\ \implies &x_1^2 - 2xx_1 + y_1^2 - 2yy_1 + z_1^2 - 2zz_1 = x_2^2 - 2xx_2 + y_2^2 - 2yy_2 + z_2^2 - 2zz_2 \\ \implies &2x(x_1 - x_2) + 2y(y_1 - y_2) + 2z(z_1 - z_2) = x_1^2 - x_2^2 + y_1^2 - y_2^2 + z_1^2 - z_2^2 \\ \implies &x(x_1 - x_2) + y(y_1 - y_2) + z(z_1 - z_2) = \frac{1}{2}(x_1^2 - x_2^2 + y_1^2 - y_2^2 + z_1^2 - z_2^2). \end{aligned}$$

Note that this is an equation of a plane. Similarly,

$$\begin{aligned} &||P_2 - C|| = ||P_3 - C|| \\ \implies &x(x_2 - x_3) + y(y_2 - y_3) + z(z_2 - z_3) = \frac{1}{2}(x_2^2 - x_3^2 + y_2^2 - y_3^2 + z_2^2 - z_3^2). \\ &||P_3 - C|| = ||P_4 - C|| \\ \implies &x(x_3 - x_4) + y(y_3 - y_4) + z(z_3 - z_4) = \frac{1}{2}(x_3^2 - x_4^2 + y_3^2 - y_4^2 + z_3^2 - z_4^2). \end{aligned}$$

We have the following system of equations:

$$\begin{cases} x(x_1 - x_2) + y(y_1 - y_2) + z(z_1 - z_2) = \frac{1}{2}(x_1^2 - x_2^2 + y_1^2 - y_2^2 + z_1^2 - z_2^2) \\ x(x_2 - x_3) + y(y_2 - y_3) + z(z_2 - z_3) = \frac{1}{2}(x_2^2 - x_3^2 + y_2^2 - y_3^2 + z_2^2 - z_3^2) \\ x(x_3 - x_4) + y(y_3 - y_4) + z(z_3 - z_4) = \frac{1}{2}(x_3^2 - x_4^2 + y_3^2 - y_4^2 + z_3^2 - z_4^2). \end{cases}$$

In [4], basic algebra (Substitution Method) was used to solve the analogous system in two dimensions. However, the algebra quickly becomes overwhelming in this scenario. Therefore, we use linear algebra theory to solve it. This system can be written as a matrix equation in the form $A\vec{x} = \vec{b}$:

$$\begin{bmatrix} (x_1 - x_2) & (y_1 - y_2) & (z_1 - z_2) \\ (x_2 - x_3) & (y_2 - y_3) & (z_2 - z_3) \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(x_1^2 - x_2^2 + y_1^2 - y_2^2 + z_1^2 - z_2^2) \\ \frac{1}{2}(x_2^2 - x_3^2 + y_2^2 - y_3^2 + z_2^2 - z_3^2) \\ \frac{1}{2}(x_3^2 - x_4^2 + y_3^2 - y_4^2 + z_3^2 - z_4^2) \end{bmatrix}.$$

To guarantee that this system has a unique solution, by Theorem 1.13 it suffices to show that

$$\det(A) = \begin{vmatrix} (x_1 - x_2) & (y_1 - y_2) & (z_1 - z_2) \\ (x_2 - x_3) & (y_2 - y_3) & (z_2 - z_3) \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) \end{vmatrix} \neq 0.$$

Remark 3.1. In $\mathbb{R}^3$, this determinant represents the scalar triple product of the vectors $\langle x_1 - x_2, y_1 - y_2, z_1 - z_2 \rangle$, $\langle x_2 - x_3, y_2 - y_3, z_2 - z_3 \rangle$, and $\langle x_3 - x_4, y_3 - y_4, z_3 - z_4 \rangle$ [8]. The absolute value of the scalar triple product represents the volume of the parallelepiped determined by the vectors. So, if we were in $\mathbb{R}^3$ we would be finished due to the three vectors being noncoplanar, thus producing a parallelepiped with volume greater than zero. (Note that if the vectors $\langle x_1 - x_2, y_1 - y_2, z_1 - z_2 \rangle$, $\langle x_2 - x_3, y_2 - y_3, z_2 - z_3 \rangle$, and $\langle x_3 - x_4, y_3 - y_4, z_3 - z_4 \rangle$ lie in the same plane, then in particular the head and tail of each vector lie in the plane which would imply that P_1, P_2, P_3, and P_4 are coplanar.) However, in $\mathbb{F}_q^3$ we have several issues to contend with. First, we are uncertain if we have a notion of volume of a parallelepiped. Second, since finite fields are unordered we would not be able to argue that the volume obtained here is greater than zero. Thus, the following argument is required.

Observe that by using row and column operations that preserve the determinant, we get:

$$\begin{aligned} \det(A) &= \begin{vmatrix} (x_1 - x_2) & (y_1 - y_2) & (z_1 - z_2) \\ (x_2 - x_3) & (y_2 - y_3) & (z_2 - z_3) \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) \end{vmatrix} \\ &\xrightarrow{R_2 + R_3 \to R_2} \begin{vmatrix} (x_1 - x_2) & (y_1 - y_2) & (z_1 - z_2) \\ (x_2 - x_4) & (y_2 - y_4) & (z_2 - z_4) \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) \end{vmatrix} \\ &\xrightarrow{R_1 + R_2 \to R_1} \begin{vmatrix} (x_1 - x_4) & (y_1 - y_4) & (z_1 - z_4) \\ (x_2 - x_4) & (y_2 - y_4) & (z_2 - z_4) \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) \end{vmatrix} \\ &= \begin{vmatrix} (x_1 - x_4) & (y_1 - y_4) & (z_1 - z_4) & 1 \\ (x_2 - x_4) & (y_2 - y_4) & (z_2 - z_4) & 1 \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix} \\ &\xrightarrow[C_3 + x_4C_4 \to C_3]{\substack{C_1 + x_4C_4 \to C_1 \\ C_2 + x_4C_4 \to C_2}} \begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{vmatrix}. \end{aligned}$$

Let B be the matrix obtained in the final step above. We have reduced the problem to showing that $\det(B) \neq 0$. For a contradiction, assume $\det(B) = 0$ and consider the system $\begin{cases} x_1a + y_1b + z_1c + d = 0 \\ x_2a + y_2b + z_2c + d = 0 \\ x_3a + y_3b + z_3c + d = 0 \\ x_4a + y_4b + z_4c + d = 0 \end{cases}$ which can be represented by the matrix equation $B \cdot \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. Since $\det(B) = 0$ it follows from Theorem 1.13 that there exists a nontrivial solution, say $a = a_0, b = b_0, c = c_0, d = d_0$ where a, b, and c are not all zero. Then $a_0x + b_0y + c_0z + d_0 = 0$ is an equation for the plane satisfied by $P_1, P_2, P_3, \text{and} P_4$, a contradiction to the fact that the four points are noncoplanar. Thus, $\det(B) = \det(A) \neq 0$ which implies A is invertible.

We now can take the inverse of A to solve for the center $\vec{x}$. For ease of notation, let

$$A = \begin{bmatrix} (x_1 - x_2) & (y_1 - y_2) & (z_1 - z_2) \\ (x_2 - x_3) & (y_2 - y_3) & (z_2 - z_3) \\ (x_3 - x_4) & (y_3 - y_4) & (z_3 - z_4) \end{bmatrix} = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}$$

and

$$\vec{b} = \begin{bmatrix} \frac{1}{2}(x_1^2 - x_2^2 + y_1^2 - y_2^2 + z_1^2 - z_2^2) \\ \frac{1}{2}(x_2^2 - x_3^2 + y_2^2 - y_3^2 + z_2^2 - z_3^2) \\ \frac{1}{2}(x_3^2 - x_4^2 + y_3^2 - y_4^2 + z_3^2 - z_4^2) \end{bmatrix} = \begin{bmatrix} \frac{1}{2}\ell \\ \frac{1}{2}m \\ \frac{1}{2}n \end{bmatrix}.$$

We have $A\vec{x} = \vec{b}$ which implies $\vec{x} = A^{-1}\vec{b}$. Thus,

$$\begin{aligned} \begin{bmatrix} x \\ y \\ z \end{bmatrix} &= \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}^{-1} \cdot \begin{bmatrix} \frac{1}{2}\ell \\ \frac{1}{2}m \\ \frac{1}{2}n \end{bmatrix} \\ &= \frac{1}{\det(A)} \cdot \begin{bmatrix} b_2c_3 - b_3c_2 & b_3c_1 - b_1c_3 & b_1c_2 - b_2c_1 \\ a_3c_2 - a_2c_3 & a_1c_3 - a_3c_1 & a_1c_2 - a_2c_1 \\ a_2b_3 - a_3b_2 & a_3b_1 - a_3b_1 & a_1b_2 - a_2b_1 \end{bmatrix} \cdot \begin{bmatrix} \ell \\ m \\ n \end{bmatrix} \cdot \frac{1}{2} \\ &= \frac{1}{2\det(A)} \cdot \begin{bmatrix} b_2c_3 - b_3c_2 & b_3c_1 - b_1c_3 & b_1c_2 - b_2c_1 \\ a_3c_2 - a_2c_3 & a_1c_3 - a_3c_1 & a_1c_2 - a_2c_1 \\ a_2b_3 - a_3b_2 & a_3b_1 - a_3b_1 & a_1b_2 - a_2b_1 \end{bmatrix} \cdot \begin{bmatrix} \ell \\ m \\ n \end{bmatrix} \\ &= \frac{1}{2\det(A)} \cdot \begin{bmatrix} (b_2c_3 - b_3c_2)(\ell) + (b_3c_1 - b_1c_3)(m) + (b_1c_2 - b_2c_1)(n) \\ (a_3c_2 - a_2c_3)(\ell) + (a_1c_3 - a_3c_1)(m) + (a_1c_2 - a_2c_1)(n) \\ (a_2b_3 - a_3b_2)(\ell) + (a_3b_1 - a_3b_1)(m) + (a_1b_2 - a_2b_1)(n) \end{bmatrix} \end{aligned}$$

Since $\det(A)$ is nonzero, this expression is well defined. We now have the coordinates for the center of a unique sphere from four distinct, noncoplanar points, which concludes our proof.

4 Zero Radius Counterexample

In [4] it was shown that three noncollinear points that are pairwise nonzero distance apart are sufficient to define a circle with nonzero radius. The crux of the argument is that in $\mathbb{F}_q^2$ there are either no zero lines or exactly two zero lines through a given point. Thus, if the three noncollinear points are all zero distance from the center C and there are at most two zero lines through C, it follows from the pigeon hole principle that at least two of the three points must lie on the same line, contradicting the hypothesis that they are noncollinear.

We originally conjectured that an analogous statement would be true for spheres. Namely, we conjectured that if $P_1, P_2, P_3, P_4 \in \mathbb{F}_q^3$ are four distinct, noncoplanar points that are pairwise nonzero distance apart, then they determine a unique sphere in $\mathbb{F}_q^3$ of nonzero radius. However, unlike the two dimensional case, it can be shown that there exist more than two zero lines in $\mathbb{F}_q^3$, so the pigeon hole principle is insufficient in this instance. We now present a counter example to this conjecture.

The following is a list of all eight zero lines in $\mathbb{Z}_7^3$ passing through the origin. It is straightforward to check that all of the points on the given lines are zero distance from each other. Figure 2 depicts ℓ_1 in $\mathbb{Z}_7^3$.

$$\begin{aligned} &\ell_1 = \{(\bar{1}t, \bar{2}t, \bar{3}t) : t \in \mathbb{Z}_7\}, \ell_2 = \{(\bar{1}t, \bar{2}t, \bar{4}t) : t \in \mathbb{Z}_7\} \\ &\ell_3 = \{(\bar{1}t, \bar{3}t, \bar{2}t) : t \in \mathbb{Z}_7\}, \ell_4 = \{(\bar{1}t, \bar{3}t, \bar{5}t) : t \in \mathbb{Z}_7\} \\ &\ell_5 = \{(\bar{1}t, \bar{4}t, \bar{2}t) : t \in \mathbb{Z}_7\}, \ell_6 = \{(\bar{1}t, \bar{4}t, \bar{5}t) : t \in \mathbb{Z}_7\} \\ &\ell_7 = \{(\bar{1}t, \bar{5}t, \bar{3}t) : t \in \mathbb{Z}_7\}, \ell_8 = \{(\bar{1}t, \bar{5}t, \bar{4}t) : t \in \mathbb{Z}_7\} \end{aligned}$$

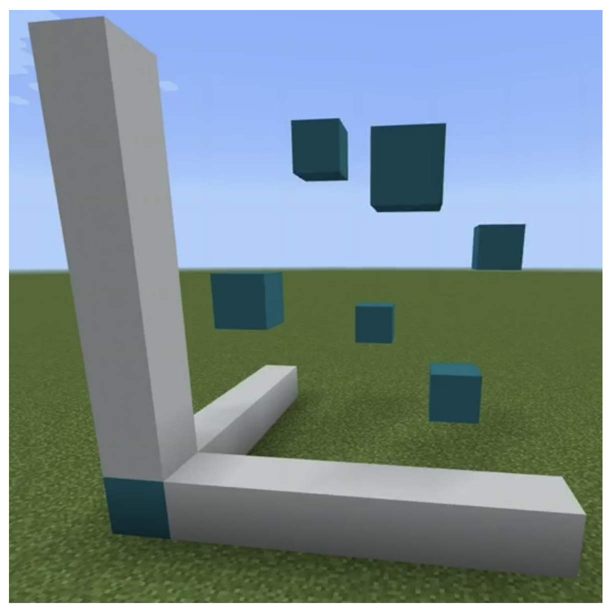

Figure 2: Zero line $\ell_1 = \{(\bar{1}t, \bar{2}t, \bar{3}t) : t \in \mathbb{Z}_7\}$. Screenshot taken from the video game *Minecraft*.

Choose four noncoplanar points that are pairwise nonzero distance apart that lie on separate zero lines from the origin. Select $P_1 = (\bar{1}, \bar{2}, \bar{3})$, $P_2 = (\bar{2}, \bar{3}, \bar{1})$, $P_3 = (\bar{3}, \bar{1}, \bar{2})$, and $P_4 = (\bar{1}, \bar{2}, \bar{4})$. Note that $P_1 \in \ell_1$, $P_2 \in \ell_8$, $P_3 \in \ell_7$ and $P_4 \in \ell_2$. We shall first verify the points are nonzero distance from each other:

$$
\begin{aligned}
||P_1 - P_2|| &= (\overline{1} - \overline{2})^2 + (\overline{2} - \overline{3})^2 + (\overline{3} - \overline{1})^2 = \overline{6} \\
||P_1 - P_3|| &= (\overline{1} - \overline{3})^2 + (\overline{2} - \overline{1})^2 + (\overline{3} - \overline{2})^2 = \overline{6} \\
||P_1 - P_4|| &= (\overline{1} - \overline{1})^2 + (\overline{2} - \overline{2})^2 + (\overline{3} - \overline{4})^2 = \overline{1} \\
||P_2 - P_3|| &= (\overline{2} - \overline{3})^2 + (\overline{3} - \overline{1})^2 + (\overline{1} - \overline{2})^2 = \overline{6} \\
||P_2 - P_4|| &= (\overline{2} - \overline{1})^2 + (\overline{3} - \overline{2})^2 + (\overline{1} - \overline{4})^2 = \overline{4} \\
||P_3 - P_4|| &= (\overline{3} - \overline{1})^2 + (\overline{1} - \overline{2})^2 + (\overline{2} - \overline{4})^2 = \overline{2}
\end{aligned}
$$

To show the points are noncoplanar, construct a plane containing P_1, P_2, and P_3 and show P_4 is not contained on the plane. We must first construct a normal vector to the plane, $\vec{n}$:

$$
\begin{aligned}
\vec{a} &= P_2 - P_1 = (\overline{1}, \overline{1}, \overline{5}) \\
\vec{b} &= P_3 - P_2 = (\overline{1}, \overline{5}, \overline{1}) \\
\vec{n} &= \vec{a} \times \vec{b} \\
&= \begin{vmatrix} i & j & k \\ \overline{1} & \overline{1} & \overline{5} \\ \overline{1} & \overline{5} & \overline{1} \end{vmatrix} \\
&= i(\overline{1} - \overline{25}) - j(\overline{1} - \overline{5}) + k(\overline{5} - \overline{1}) \\
&= \overline{4}i + \overline{4}j + \overline{4}k
\end{aligned}
$$

Now, using P_1 we get the equation of the plane to be $\overline{4}(x - \overline{1}) + \overline{4}(y - \overline{2}) + \overline{4}(z - \overline{3}) = \overline{0}$ or $\overline{4}x + \overline{4}y + \overline{4}z + \overline{4} = \overline{0}$. To see that P_4 is not contained in the plane, observe that $\overline{4}(\overline{1}) + \overline{4}(\overline{2}) + \overline{4}(\overline{4}) + \overline{4} = \overline{4} + \overline{1} + \overline{2} + \overline{4} = \overline{4} \neq \overline{0}$. Thus, P_1, P_2, P_3 and P_4 are noncoplanar.

However, $C = (\overline{0}, \overline{0}, \overline{0})$ satisfies $||P_1 - C|| = ||P_2 - C|| = ||P_3 - C|| = ||P_4 - C|| = \overline{0}$ which shows that C is the center of the sphere of radius $\overline{0}$ containing the points P_1, P_2, P_3 and P_4. Figure 3 depicts a representation of this particular sphere in $\mathbb{Z}_7^3$.

Therefore, four noncoplanar points that are nonzero distance apart is not sufficient to guarantee a sphere with nonzero radius.

5 Conclusion and Further Research

We have shown that in $\mathbb{F}_q^3$, four distinct, noncoplanar points pairwise nonzero distance apart determine a unique sphere. Extending this finding into higher dimensions would be the first logical next step in this topic of research, as well as finding novel methods of representing these spheres. An exploration of zero lines in general is also warranted as little is known about their properties outside their defining characteristic. Specifically, the researchers would like to examine the cardinality of zero lines in $\mathbb{F}_q^n$, as well as determining the conditions of their existence in lower dimensions.

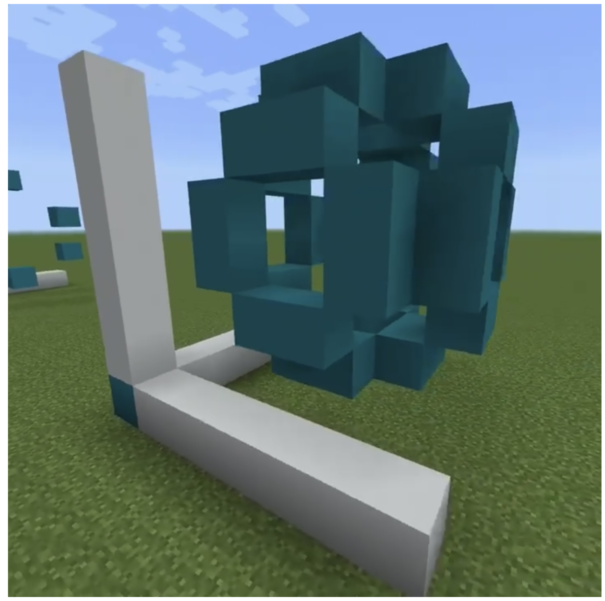

Figure 3: A sphere of radius zero centered at $(\overline{0}, \overline{0}, \overline{0})$ in $\mathbb{Z}_7^3$. Notice in this case the center is in fact included as a part of the sphere. Screenshot taken from the video game *Minecraft.*

6 Acknowledgments

We are sincerely grateful to the referees for their thorough review of our paper. Their thoughtful comments undoubtedly added to its quality.

References

[1] Axler, Sheldon. *Linear Algebra Done Right.* 2nd ed. Springer-Verlag New York, Inc., 1997,1996. Print.

[2] Euclid. *The Elements Book IV.* Trans. Sir Thomas L. Heath. NewYork: Dover, 1956. Print.

[3] Gilbert, Jimmie, and Gilbert, Linda. *Elements of Modern Algebra.* 6th ed. Belmont: Thomson Books/Cole, 2005. Print.

[4] J. Haddock, W. Perkins, J. Pope, and J. Chapman. *Circles in* $\mathbb{F}_q^2$. Aletheia, Vol. 2 (1), 2017.

[5] Larson, Ron, and Falvo, David. *Elementary Linear Algebra.* 6th ed. Houghton Mifflin, Inc., 2009. Print.

[6] Lidl, Rudolf, and Niederreiter, Harald. *Finite Fields.* Cambridge University Press, 1997. Print.

[7] Phuong, Nguyen Duy, Pham, Thang, Sang, Nguyen Minh, Valculescu, Claudiu, and Vinh, Le Anh. *Incidence Bounds and Applications Over Finite Fields.* arXiv:1601.00290 [math.CO], 2016.

[8] Stewart, James. *Calculus Early Transcendentals.* 8th ed. Cengage Learning, 2016, 2012. Print.