FINITE PROJECTIVE PLANES AND QUADRATIC FORMS WITH APPLICATIONS

XINKAI WU

ABSTRACT. In this paper, we shall examine the connections between quadratic forms and combinatorial objects, such as finite projective plane. We will explain the algebraic structure associated with a finite projective plane. In particular, we aim to show a short proof of the Bruck-Ryser theorem which concerns with the non-existence of orders of finite projective plane using the arithmetic of quadratic forms. We will also explore other combinatorial applications of quadratic forms, such as the "eventown clubs" problem. Finally, we shall explain how to apply these concepts to coding theory using Smith normal form and quadratic forms which in turn tells us more about the properties of finite projective plane. We shall assume knowledge of elementary number theory in addition to some familiarity with linear algebra.

CONTENTS

1. Quadratic Space and Combinatorial applications 1
2. The Bruck-Ryser Theorem 3
3. Smith Normal Form with Applications in Coding Theory 8
Acknowledgments 12
References 12

1. QUADRATIC SPACE AND COMBINATORIAL APPLICATIONS

Definition 1.1. (*Symmetric Bilinear Form*)We call a map B: $V \times V \to F$ (V a vector space over field F) a *symmetric bilinear form* if it satifies the following conditions:
1) $B(x, y) = B(y, x)$.
2) $B(x, y + z) = B(x, y) + B(x, z)$ and $B(x + y, z) = B(x, z) + B(y, z)$.
3) $B(ax, y) = aB(x, y), B(x, ay) = aB(x, y)$.

We call a vector space V a *quadratic space* if we have a symmetric bilinear form B associated with V.

We call a map Q a *quadratic form* induced by a symmetric linear form if $Q(x) = B(x, x) \in F$.

We can introduce the notions of orthogonality and basis in the same way as we have defined them in linear algebra.

Definition 1.2. (*Orthogonal complement*) We call a subspace $S^{\perp}$ the *orthogonal complement of a subspace* S in a quadratic space V equipped with a quadratic form Q if for all $v \in S^{\perp}$ and $u \in S$ we have $Q(v, u) = 0$.

Furthermore, we call a subspace U *totally isotropic* if $U \subseteq U^{\perp}$.

We call a quadratic space V *non-singular* if $V \cap V^{\perp} = 0$.

Theorem 1.3. *(Dimension Formula)*

For all non-singular quadratic spaces V, and for any subspace S in V, we have the dimension formula: $\dim(V) = \dim(S) + \dim(S^{\perp})$.

Proof. See Babai's book [2,54].

□

Hence we can easily obtain the following theorem.

Theorem 1.4. *(Maximal Dimension)*

Suppose we have a non-singular vector space V of dimension n. Then all the totally isotropic subspaces of V have dimension at most $\lfloor \frac{n}{2} \rfloor$.

Proof. Suppose U is a totally isotropic subspace. Then $U \subseteq U^{\perp}$ implies that $\dim(U) \leq \dim(U^{\perp})$. By Theorem 1.3, $\dim(U) + \dim(U^{\perp}) = n$ is at least 2 times $\dim(U)$. Therefore, $\dim(U) \leq \lfloor \frac{n}{2} \rfloor$.

□

Now we turn to a classical combinatorial question.

Consider a town with n citizens. They can form arbitrarily many clubs they like satisfying the following two rules:

1) Each club has an even number of members.

2) The intersection of every two distinct clubs is even.

Suppose the number of clubs is m. What is the upper bound of m?

Before we give the upper bound, we first demonstrate that m can achieve very large values. We simply group the n citizens into $\lfloor \frac{n}{2} \rfloor$ groups with 2 members in each group. By considering the power set of these 2-members groups, we find that there are $2^{\lfloor \frac{n}{2} \rfloor}$ many ways to union them. It is clear that all the unions of these 2-person groups satisfy the eventown rules. Hence the upper bound of m is at least exponentially large. It is interesting to compare this result with other rules of forming clubs. If there is no restriction on forming clubs, then we can form precisely 2^n many clubs, i.e, the number of possible subsets of these n citizens. However, if the clubs satisfy the "oddtown rules", such that each club contains even number of people and each intersection of any two clubs is odd, then $m \leq n$. A proof of this result also uses linear algebra methods. The reader can check the beginning of Babai's book [2,1] for details.

Now we prove a simple lemma.

Theorem 1.5. *The space F_2^n, an n-dimensional vector space over finite field F_2, is non-singular under the standard inner product.*

Proof. Consider a vector in F_2^n, where $v = (v_1, \ldots, v_n), v_i \in \{0, 1\}$, and not all v_i are 0. If v contains odd number of 1, then v is not perpendicular to any vector with odd number of 1, as their inner product is 1 in F_2. If v contains even number of 1, then we can construct a vector u such that u contains all but one 1 in the same position. Then $u \cdot v = 1$. Hence,there is no vector besides 0 that is perpendicular to all vectors in F_2^n. Hence F_2^n is non-singular. □

Now we are ready to show the main theorem.

Theorem 1.6. *The tight upper bound of m is $2^{\lfloor \frac{n}{2} \rfloor}$.*

Proof. The tightness is shown in previous constructive example. Now we need to show $m \leq 2^{\lfloor \frac{n}{2} \rfloor}$.

Consider the incidence vectors of all the clubs. That is, we represent each club by an n-dimensional vector over finite field F_2. The i^{th} position of the incidence vector is 0 if the i^{th} citizen is not in the club, and 1 otherwise.

Consider the subspace U of the span of these incidence vectors inside F_2^n. We define a quadratic form on F_2^n using the standard inner product, $Q(v, u) = \sum v_i \cdot u_i$.

Now we claim that U is totally isotropic. We note that $v \cdot u$ is the number of citizens in the intersection of club v and club u. Hence, $v \cdot u$ is even, which means they are orthogonal in U. Hence, U is totally isotropic.

By Theorem 1.4, $dim(U) \leq \lfloor \frac{n}{2} \rfloor$. Thus, the number of vectors $m \leq 2^{\lfloor \frac{n}{2} \rfloor}$.

This concludes the tight upper bound of m is $2^{\lfloor \frac{n}{2} \rfloor}$.

□

The method presented in this section can be extended to various other combinatorial questions. See [2] for details.

2. The Bruck-Ryser Theorem

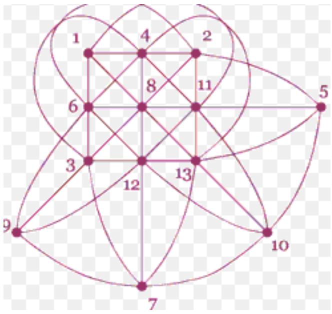
Now we are going to connect the combinatorial question of finite projective planes with quadratic forms.

Definition 2.1. (*Finite Projective Plane*)

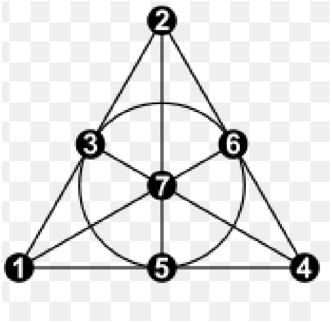
A *Finite Projective Plane* is a set system consisting points and lines in which every two points belong to exactly one line and every two lines intersect at exactly one point. Furthermore, there are four points in the plane such that no three points in these four points are collinear.

We can demonstrate that a finite projective plane contains N points and N lines which means the number points equal to the number of lines. Furthermore, all lines contain the same number of points, and every point is on the same number of lines. Furthermore, the number of points on a line equals the number of lines passing through a point. If this number is $n + 1$, then $N = n^2 + n + 1$. We call n the order of the finite projective plane. It is conjectured that n has to be prime. For details, the reader can check [2].

Below is an example of a finite projective plane with order 3.



The most famous finite projective plane is the Fano plane which has order 2.



In fact, we can construct a finite projective plane if its order n is a power of prime. If n is a power of prime, then we can construct a finite field K of order n. Consider the partition(projectivization) of $K^3 - \{0\}$, $(K^3 - \{0\})/(\sim)$, in which $[a, b, c] \sim [wa, wb, wc]$ for all non-zero scalar w in K. $\sim$ is an equivalence relation, so the partition is well defined. There are $\frac{n^3-1}{n-1} = n^2 + n + 1$ many equivalence classes in this partition. We label these elements as the points and lines of our plane. Each point or line is in the form of $[a, b, c]$.We call a point p incident to a line l if $p \cdot l = 0$, that is $[a, b, c] \cdot [x, y, z]^t = 0$. Such construction satisfies all the axioms of being a finite projective plane. Hence, for any given power of prime, we can construct an associated finite projective plane, which people usually denote as the *Galois Plane of order n.*

The converse of this statement that whether an order has to be a power of prime is much harder.

It is oftentimes convenient to consider the incidence matrix A of a projective plane. An incidence matrix A of a projective plane is a $N \times N$ matrix such that

$$(a_{ij}) = \begin{cases} 1 & \text{if point } i \text{ is on line } j \\ 0 & \text{otherwise} \end{cases} \tag{2.2}$$

We can verify that

$$A^tA = B = \begin{pmatrix} n+1 & 1 & 1 & \cdots & 1 \\ 1 & n+1 & 1 & \cdots & 1 \\ 1 & 1 & n+1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & n+1 \end{pmatrix}. \tag{2.3}$$

Since any two lines meet at exactly one point, the off-diagonal elements are 1, and each line contains precisely $n + 1$ points, so the diagonal elements are $n + 1$. Therefore, for a finite projective plane of order n to exist, there needs to be a corresponding matrix A such that $A^tA = B$. The existence of such A is equivalent to the existence of the corresponding projective plane.

In order to fully extract information of invariants of the matrix from the above constraint, we will employ tools from quadratic forms.

See [1, Chapter 3] for a detailed treatment of p-adic numbers and more. In particular, we shall assume that the readers are familiar with the basic definitions of $\mathbb{Q}_p$. For completeness, we shall make some short definitions.

Definition 2.4. (*p-adic metric*) For $a = 0$, define $|a|_p = 0$.

For any nonzero rational number $a = \frac{b}{c}$ in which $gcd(b, c) = 1$, define its p-adic norm as $|a|_p = \dfrac{1}{\operatorname{ord}_p(b) - \operatorname{ord}_p(c)}$, in which $\operatorname{ord}_p(b)$ is the exponent of p in the factorization of b. Then it induces a p-adic metric $d(x, y) = |x - y|_p$, as every norm induces a natural metric.

As every metric space has a completion, we define the completion of Q under this p-adic metric as $\mathbb{Q}_p$.

Definition 2.5. (*Hilbert Symbol*)
In $\mathbb{Q}_p^\times$, we define

$$(a, b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ is solvable in } \mathbb{Q}_p \\ -1 & \text{otherwise .} \end{cases} \tag{2.6}$$

We will only state some important propositions of Hilbert symbol without proving them, as our task is to use them for proving the Bruck-Ryser theorem. These referenced results will only be used in the calculation of the incidence matrix later.
1)$(a, bc)_p = (a, b)_p \cdot (a, c)_p, (ab, c)_p = (a, c)_p \cdot (b, c)_p$.
2)$(a, b)_p = 1 \forall a = k^2 \in \mathbb{Q}_p$.
3)$(a, b)_p = (b, a)_p$.
For proof of the above propositions, see [1, Chapter 4].
We also need more knowledge about quadratic spaces.

Definition 2.7. (*Regular Quadratic Space*) Suppose we have a quadratic space V. If $V^\perp = \{0\}$, then we call V a *regular quadratic space.*

Like in linear algebra, for any quadratic space (V, B) with an associated symmetric billinear form B, we have an orthogonal basis associated with it. See [1, 17].
Each quadratic space (V, B) with symmetric billinear form B has a natural Gram matrix associated to it. We call the matrix $(a_{ij}) = B(e_i, e_j)$ in which e_i is a basis of V the *Gram matrix* of V.

Definition 2.8. (*Hasse Symbol*)
Suppose we have an orthonomal basis (a_i) for a regular quadratic space V, then we define the *Hasse Symbol* of V as $S_pV = \prod_{i<j}(a_i, a_j)_p$, a product of Hilbert Symbols. .

Fortunately, the value of Hasse symbol doesn't depend on what orthogonal basis we choose. See [1, 86, Proposition 4.17] for proof.

Theorem 2.9. *The value of the Hasse symbol remains the same under isometry.*

Proof. For proof, see [3, 115, Proposition 3.18]. □

We now state the formal definition of isometry for completeness. For a detailed treatment of related content, see [3, Chapter 1].

Definition 2.10. (*Isometry of Quadratic Spaces*)
We call two quadratic spaces (V, p) and (U, q), with quadratic forms p and q, *isometric* if there is an invertible linear map T between them such that $p(v) = q(Tv)$ for all v in V.

Equivalently, an isometry between two quadratic spaces corresponds to a matrix congruence. We call two matrices A and B congruent if there is some invertible matrix P such that $A = P^t BP$. Two quadratic spaces are isometric if their underlying Gram matrices are congruent. The reason of this correspondence is that any two congruent matrices represent the same quadratic form under change of basis. Therefore, Hasse symbol is invariant under matrix congruence.

Now we are ready to state and prove the Bruck-Ryser theorem.

Theorem 2.11. *(The Bruck-Ryser Theorem)*
Suppose $n \equiv 1$ *or* $2 \pmod 4$*, and it is the order of some finite projective plane. Then n is a sum of two squares.*

Proof. By Fermat's theorem of sums of two squares, an integer n is a sum of two squares if and only if its prime factors p such that $p \equiv 3 \pmod 4$ have even exponents, which means $\mathrm{ord}_p(n)$ is even.

We construct a matrix F to help our analysis.

$$F = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ n^{-1} & 1 & 0 & \cdots & 0 \\ n^{-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n^{-1} & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{2.12}$$

Construct another matrix K such that its diagonal elements are $< 1, n, n..., n >$.

This construction forces that $S^t KS = B$ which means B and K are congruent matrices. However, note that $A^t A = B$, so the identity matrix is another diagonalization of B. Hence, we have an isometry of the two regular quadratic spaces V, W characterized by matrices $< 1, n, n, n, \dots, n >$ and $< 1, 1, \dots, 1 >$. Hence, by previous theorem about the invariance of Hasse symbols, we conclude that

$$S_p V = S_p W. \tag{2.13}$$

As V is characterized by the identity matrix, its Hasse symbol is simply 1.

On the other hand, W is characterized by $< 1, n, n, n, \dots, n >$, hence

$$S_p W = (1, n)_p \cdot \prod_{i<j} (n, n)_p = \prod_{i<j} (n, n)_p.$$

There are $\binom{N-1}{2}$ many unordered pairs of $(n, n)_p$, therefore,

$$S_p W = (n, n)_p^{\binom{N-1}{2}} = (n, -1)_p^{\frac{(N-1)(N-2)}{2}}.$$

We are given that $n \equiv 1, 2 \pmod 4$, which forces $N = n^2 + n + 1 \equiv 3 \pmod 4$. Thus, $\frac{(N-1)(N-2)}{2} \equiv 1 \pmod 2$.

The exponent is odd, so it doesn't change the sign of $(n, -1)_p$.

We have,

$$S_p W = (n, -1)_p = S_p V = 1$$

Suppose p is any prime factor of n such that $\mathrm{ord}_p(n)$ is odd, we want to show that $p \equiv 1 \pmod 4$.

Suppose $n = p^{2k+1} u$, where $2k + 1 = \mathrm{ord}_p(n)$.

Then

$$1 = (n, -1)_p = (p, -1)_p \cdot (u, -1)_p = (\frac{-1}{p}). \tag{2.14}$$

by properties of Hilbert symbol.

Here, $(\frac{-1}{p})$ is the Legendre symbol.

From elementary number theory, we know that -1 is a square in F_p if and only if $p \equiv 1 \pmod 4$.

Then, by the Fermat's theorem of sums of two squares we mentioned previously, n is a sum of two sqaures.

This concludes the proof of Bruck-Ryser theorem.

□

The above proof using quadratic forms uses more machinery than that is used in Bruch and Ryser's original paper, however, it has the benefit of being more concise and comprehensible, as the original proof is quite involved with more artificial construction. We encourage the reader to read the original paper and various other proofs of this theorem.

Note that the Bruck-Ryser theorem is only a necessary condition. For instance, $10 \equiv 2 \pmod 4), 10 = 1^2 + 3^2$, which satisfies the conditions of Bruck-Ryser. However, it has been shown that order 10 doesn't exist. The proof relies on techniques from coding theory, as well as a computer search. For an overview of this proof, see [4]. We will also give a brief review of that proof in the next section which largely follows from L.Babai's exercises.

Before we explore topics of coding theory, we will end the section by pointing out some other important algebraic structures of finite projective plane.

Definition 2.15. (*Collineation*) We call a bijection between two finite projective plane a *collineation* if it preserves the incidence relation between points and lines, which means it sends collinear points to collinear points.

We can then define all the collineations (automorphisms) of a finite projective plane as a *collineation group* in which the group operation is the composition between the collineation.

Theorem 2.16. *The collineations of any finite projective plane form a group under composition.*

Proof. Closure is apparent as the composition of collineations still preserves the original incidence relation. Associativity is inherited as composition of functions is associative. Any collineation is bijective, so each collineation p naturally inherits an inverse p^{-1} which again preserves incidence relation as incidence relation is a dual property. □

As we have a group structure associated to a finite projective plane, we can get more information about the finite projective plane and its order by analyzing its group structure more carefully. For details, see the survey article [6].

Theorem 2.17. *The collineation group of the Fano plane is order 168.*

Proof. Suppose we have labelled the Fano plane with numbers $1, 2, 3, 4, 5, 6, 7$ in a way that 1,2,3 are collinear. Suppose we have a collineation p. There are 7 choices for $p(1)$. There are then 6 ways to choose $p(2)$. p preserves incidence relation, so the third point $p(3)$ must lie on the lines formed by $p(1)$ and $p(2)$. Then there are 4 positions left for $p(4)$. The rest points are determined due to incidence relation with previous points. Hence, there are $7 \cdot 6 \cdot 4 = 168$ many distinct collineations. □

If we have a bit familiarity with finite group theory, we will be able to recognize that the projective general linear group $PGL(2,7) \simeq PSL(2,7)$ is also of order 168. In fact, $PSL(2,7) \simeq GL(3,2)$ acts on the Fano plane by the usual fractional linear transformation. Furthermore, this induced group action makes the $PSL(2,7)$ an isomorphic subgroup of the collineation group of the Fano plane.As they have the same order, we can conclude that $PSL(2,7) \simeq Aut(P)$ in which we denote the collineation group of the Fano plane as $Aut(P)$.

3. Smith Normal Form with Applications in Coding Theory

Many ideas of this section come from the author's notes in Laci Babai's 2020 course on combinatorics.

We begin by giving some definitions in coding theory.

Definition 3.1. ($[n,k]$ *code*)

We call a k-dimensional vector subspace in F_q^n over finite field F_q a $[n,k]$ *code.*

Recall our definition of orthogonal complement of vector space. We call a code C a self-dual code if $C = C^{\perp}$.

By Theorem 1.3, we have $\dim(C) + \dim(C^{\perp}) = n$. It follows that if C is a $[n,k]$ code, then $C^{\perp}$ is always a $[n, n-k]$ code.

Now we can try to relate projective plane with codes. From now on, we assume that the order of finite projective plane is even.

Definition 3.2. (*Augmented incidence matrix*)

Consider the $N \times N$ incidence matrix of some finite projective plane A. Consider the sum of elements in the i^{th} row which we denote as s_i. If s_i is even, then we add a 0 to the end of row i. If s_i is odd, then we add a 1 to the end of row i. This new $N \times (N+1)$ matrix is called the *augmented incidence matrix* of A.

Now consider the subspace U with the basis as the rows of the augmented incidence matrix A' of A.

Suppose n is even. The sum of all columns of A is a column vector $(1, 1, \dots, 1)^t$ as $n + 1 = 1$ in F_2, so that the extra column is a linear combination of previous columns.

Hence, the rank of A and the rank of A' are the same when n is even.

Theorem 3.3. *The subspace of F_2^{N+1} spanned by the rows of the augmented matrix, U, is totally isotropic.*

Proof. n even implies that $N = n^2 + n + 1$ is odd, which means we must add 1 to the end of each row of the original matrix to make the sum even.

Any two rows of the incidence matrix can only have exactly one 1 in common because two points uniquely determine a line in a projective plane.

The inner product of any two rows is precisely the number of common points they share.

Therefore, for any two rows of the augmented matrix, $a_i \cdot a_j = 1 + 1 = 0$ as the last column of the augmented matrix is all one. Furthermore, $a_i \cdot a_i = n + 2 = 0$ as each line contains precisely $n + 1$ many points.

For any two vectors a and b spanned by the rows a_i, b_i, we have, by distributivity, $a \cdot b = \sum a_i \cdot \sum b_i = \sum \sum a_i \cdot b_j = 0$.

This concludes that U is totally isotropic. □

We also need some results from determinants and Smith normal form to proceed.

Theorem 3.4. *Suppose we have a matrix $A = (a_{ij})$ in which the diagonal elements $a_{ii} = b$ and the off-diagonal elements $a_{ij} = a$. Then*

$$\det(A) = (a-b)^{n-1}(a+(n-1)b)$$

.

Proof. Add all the rows to the first rows, we will get a new first row $(a_{1j}) = a + (n-1)b$.

Take the cofactor of $a + (n-1)b$ out. We get,

$$A' = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a \end{pmatrix}. \tag{3.5}$$

It follows that $\det(A) = (a + (n-1)b) \cdot \det(A')$.

Replace each a_i with $a_i - b \cdot a_1$, we get

$$A'' = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & a-b & 0 & \cdots & 0 \\ 0 & 0 & a-b & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a-b \end{pmatrix}. \tag{3.6}$$

Hence, $\det(A) = (a + (n-1)b)(a-b)^{n-1}$.

□

The above determinant formula is not only useful in our next discussion of coding theory, but also in combinatorics. For instance, it can be used to prove the *Generalized Fisher inequality.* We give a brief explanation of that inequality to demonstrate the usefulness of this determinant formula.

Theorem 3.7. *Suppose we have m many distinct subsets in a universe of n elements with the pairwise intersection. Then we claim that $m \leq n$.*

The reader will notice that this theorem has a similar flavor of the eventown problem we have considered previously. Here the pairwise intersection is the intersection of any two sets in the universe, while the pairwise intersection is the intersection of any two clubs in the eventown problem.

Proof. Consider the Gram matrix G of the incidence vectors of these m many subsets. By the determinant formula proven above, we have $\det(G) \neq 0$. Hence, it is non-singular. If the Gram matrix is non-singular, then its associated vectors are linearly independent. There are at most n linearly independent vectors in R^n, so $m \leq n$. □

We now give some basic results about Smith normal form.

Definition 3.8. (*Smith normal form*) We call a matrix A over $\mathbb{Z}$ in *Smith normal form* if $a_{11}|a_{22}|a_{33}\ldots$, which means any diagonal element in the matrix(not necessarily a square matrix) divide the following ones. The off-diagonal elements are all 0.

Definition 3.9. (*Determinantal divisor*) We call the greatest common divisor of all the $j{\cdot}j$ minors of A (the intersection of j rows and j columns) the j-th *determinantal divisor*of A, denoted $d_j(A)$.

We then denote the j^{th} invariant factor as $\dfrac{d_j(A)}{d_{j-1}(A)}$ as $a_j(a)$.

We call a matrix A unimordular if $\det(A) = 1$ or -1.

The Smith normal form theorem (See Steven's notes [7] for proof) implies that, for any matrix A over Z, there are two unimodular matrices K and L such that $rk(A) = rk(KAL)$, and KAL is the unique smith normal form of A in which they share the same invariant factors.

We can use this theorem to deduce a theorem regarding the determiant of matrix.

Theorem 3.10. *Suppose A is a square matrix over integer, and we denote $rk_p(A)$ as the rank of the matrix of A mod p (A over F_p), then $p^{n-rk_p(A)}$ divides* $\det(A)$ *over integers.*

Proof. If $\det(A) = 0$, then the statement holds.

Otherwise, suppose A non-singular. Applying Smith normal form theorem, there are some unimodular matrices, denoted as K and L, such that $B = KAL$ is in Smith normal form. Furthermore, $rk(KAL) = rk(B) = rk(A)$ over $\mathbb{Z}$, B and A have the same invariant factors.

In F_p, $\det_p(K) = \det_p(L) = 1 \pmod p = 1$, so $rk_p(B) = rk_p(A)$ over F_p as well, since K, L are non-singular in F_p. $\det(B) = \det(KAL) = \det(A)$ in F_p.

We have $B = (b_{ij} \pmod p) = diag(b_{ii} \pmod p)$. If $rk_p(B) = k$, then $n-k$ many columns in B in F_p are linearly dependent, which means $n-k$ many diagonal entries are 0. Hence, there are $n-k$ many diagonal entries in B divisible by p in B over the integers. $\det(B) = \prod b_{ii} \implies p^{n-k} \mid \det(B) = \det(A)$. □

Now we are getting closer to apply coding theory to finite projetcive plane.

Assume further that $n \equiv 2 \pmod 4$.

Theorem 3.11. *If $n \equiv 2 \pmod 4$, then the subspace U formed by the rows of the augmented incidence matrix has the property that $U = U^{\perp}$.*

Proof. We need to show that $\dim(U) = \frac{N+1}{2}$.

Let I be the incidence matrix of the projective plane A and I' be the augmented matrix. The augmented matrix has an extra all one column in the end as we have reasoned in Theorem 3.3.

We have $I \cdot I^T = B$ in which B is the all one matrix plus n times the identity matrix.

Over $\mathbb{Z}$, by Theorem 3.4,

$$\begin{aligned}\det(I)^2 &= \det(I \cdot I^t)\\ &= n^{n^2+n+1-1}(n+1)^2\\ &= (n+1)^2 \cdot n^{n^2+n}\end{aligned}$$

which implies that $\det(I) = (n+1) \cdot n^{\frac{n^2+n}{2}}$.

We are given that $n \equiv 2 \pmod 4$. Hence, $2 \mid n+1$ and $4 \nmid n$, which implies $\mathrm{ord}_2(\det(I)) = \frac{n^2+n}{2}$.

Then, by Theorem 3.10, over F_2, $(p^{N-rk_2(I)}) \mid \det(I)$ which implies that

$$N - rk_2(I) \leq \frac{n^2+n}{2}.$$

Then $rk_2(I) \geq \frac{N+1}{2}$. Hence, $rk_2(I') \geq \frac{N+1}{2}$.

By Theorem 1.4, we must have $rk_2(I') = \frac{N+1}{2}$, which implies that $\dim(U) = \frac{N+1}{2}$.

This concludes the proof. □

Codewords play a central role in reducing how much computer search one should do.

Definition 3.12. (*Weight enumerator of codeword*) The weight of a vector is the number of its non-zero coordinates. We denote w_i as the number of vectors in F_p^n that have i weight. We call W a weight enumerator for some vector space K over F_p by $W_K(x,y) = \sum_{i=0}^{n} w_i x^{n-i} y^i$.

An important identity that was discovered by MacWilliams tells us that

$$W_K(x,y) = \frac{1}{2^k} W_{K^\perp}(x+y, x-y) \tag{3.13}$$

in which K is a k dimensional subspace of F_2^n. For proof and more details about error correcting codes, see MacWilliams' book [5].

We will finally explain why our previous work is related to this theorem.

Our vector subspace U, as constructed as the span of augmented matrix, is maximally isotropic with dimension $\frac{N+1}{2}$ when $n \equiv 2 \pmod 4$. Hence, the MacWilliams identity becomes

$$W_K(x,y) = \frac{1}{2^{\frac{N+1}{2}}} W_{K^\perp}(x+y, x-y). \tag{3.14}$$

When $n = 10$, we should have $\dim(U) = \frac{112}{2} = 56$, so the equation becomes

$$W_K(x,y) = \frac{1}{2^{56}} W_{K^\perp}(x+y, x-y). \tag{3.15}$$

Thus, it is expected that many incidence relations of points and lines don't satisfy the above constraints. Hence, we no longer need to check all the possible $(0,1)$ matrices of order N. For details of how to actually eliminate these matrices, see the papers in [4] and [6].

The above coding theoretic approach to prove the non-existence of other orders is limited as it seems hard to be generalized. There are other algebraic approaches to the general case by analyzing the collineation group associated with a finite projective plane.

Acknowledgments

It is a pleasure to thank my mentor, Xingyu Wang, for providing helpful feedback on revising the paper and making insightful suggestions. I also thank the director of this REU program, Peter May, for organizing the REU during this hard time. I also thank L.Babai for his wonderful class on combinatorics. I am also grateful for Minh-Tam who introduces to me the topics of finite projective plane in the Directed Reading Program.

References

[1] Larry.J.Gerstein. Basic Quadratic Forms. American Mathematical Society GSM Volume 90.

[2] L.Babai.Linear Algebra Methods in Combinatorics. http://people.cs.uchicago.edu/ laci/CLASS/HANDOUTS-COMB/BaFrNew.pdf

[3] T.Y.Lam. Introduction to Quadratic Forms over Fields. American Mathematical Society GSM Volume 67.

[4] C.W.H.Lam, L.Thiel, and S.Swiercz. The nonexistence of code words of weight 16 in a projective plane of order 10. Journal of Combinatorial Theory, Series A, 1986 - Elsevier.

[5] F.J MacWilliams, N.J.A. Sloan. The theory of Error-Correcting Codes. North-Holland Publishing Company (1977).

[6] Dominique J.Roy. Confirmation of The Non-Existence of a Projective Plane of Order 10. Masters Thesis in the Ottawa-Carleton Institute.

[7] Steven V.Sam. http://www.math.wisc.edu/ svs/490/SNF.pdf