1 Appendix

Proposition 1.1

$(V, \mathscr{B})$ is an (v, b, r, k, λ)-BIBD iff its incidence matrix N satisfies the following conditions:

1. *$N 1_b = r 1_v$, where 1_b is the column vector of size b contains all 1, and 1_r is the column vector of size 4 contains all 1.*
2. *$1_v^T N = k 1_b^T$ where 1_v^T is transpose.*
3. *$NN^T = (r - \lambda)\mathrm{Id}_v + \lambda\lambda J_v$ where J_m is the $m \times m$ matrix contains all 1.*

Proof.

$$N 1_b = \begin{bmatrix} \sum_{j=1}^{b} N_{1j} \\ \vdots \\ \sum_{j=1}^{b} N_{vj} \end{bmatrix}$$

and so $N 1_b = r 1_v$ iff $\sum_{j=1}^{b} N_{ij} = r$ for all $i = 1, \ldots, v$ iff x_i lies in exactly r blocks for all i.

Similarly, $1_v^T N = k 1_b^T$ iff each block has k points.

Finally, consider NN^T. We see $(NN^T)_{ii}$ is equal

$$\sum_{j=1}^{b} N_{ij} N_{ij}^T = \sum_{j=1}^{b} N_{ij}^2 = \sum_{j=1}^{b} N_{ij}$$

So $(NN^T)_{ii} = r$ for all i iff the first condition holds.

For $i \neq j$, we see

$$(NN^T)_{ij} = \sum_{l=1}^{b} (N_{il})(N^T)_{lj} = \sum_{l=1}^{k} N_{il} N_{jl}$$

where in the last sum, it is equal 1 iff x_i and x_j are both in α_l. Hence, the last sum is the number of blocks containing both x_i and x_j. Thus $(NN^T)_{ij} = \lambda$ iff every pair of distinct points lies in λ many blocks.

Thus (1) to (3) are equivalent to the three conditions defining a BIBD.

Lemma 1.2

The incidence matrix N of a symmetric design is normal (i.e. $NN^T = N^T N$).

Proof. We have $NJ = JN$ where we set $J = J_v$. Indeed, we see $NJ = N1_v1_v^T = r1_v1_v^T = rJ$ and on the other hand $JN = 1_v1_v^T N = k1_v1_v^T = kJ = rJ$.

Now consider

$$\begin{aligned} NNN^T &= N((r-\lambda)I + \lambda J) \\ &= ((r-\lambda)J + \lambda I)N \\ &= N(N^T N) \end{aligned}$$

Now multiply both side by N^{-1} we conclude $NN^T = N^T N$ as desired.

Recall the order of a design is $n = r - \lambda$. Now suppose the design is symmetric, then

$$n = r - \lambda = k - \lambda$$

and hence the above lemma tells us

$$NN^T = N^T N = nI + \lambda J$$

Proposition 1.3

If a symmetric (v, k, λ)-design exists, then $I_v \approx_{\mathbb{Q}} nI_v + \lambda J_v$ where $n = k - \lambda$.

Proof. We know $N \in M_{n\times n}(\mathbb{Q})$ is invertible and

$$N^T I_v N = N^T N = nI_v + \lambda J_v$$

Here is some basic properties of congruence.

Proposition 1.4

1. *$\approx_{\mathbb{Q}}$ is an equivalence relation.*
2. *If we have $A = \mathrm{Diag}(A_1, \ldots, A_s)$ is a matrix with block matrices on the diagonal, then $A \approx_{\mathbb{Q}} \mathrm{Diag}(A_{\sigma(1)}, \ldots, A_{\sigma(s)})$ with $\sigma \in S_s$.*
3. *If $A \approx_{\mathbb{Q}} B$ and $B = B^T$ then $A = A^T$.*
4. *If $A \approx_{\mathbb{Q}} B_i$ for $i = 1, \ldots, s$, then $\mathrm{Diag}(A_1, \ldots, A_s) \approx_{\mathbb{Q}} \mathrm{Diag}(B_1, \ldots, B_s)$.*

Proof. Exercise!

The notion of congruence is also related to bilinear forms.

Definition 1.5

Let V be a vector space over $\mathbb{Q}$, a ***bilinear form*** on V is a map $\alpha : V \times V \to \mathbb{Q}$ such that:

1. $\alpha(x + ty, z) = \alpha(x, z) + t\alpha(y, z)$
2. $\alpha(x, y + tz) = \alpha(x, y) + t\alpha(x, z)$

for all $x, y \in V$ and $t \in \mathbb{Q}$.

Definition 1.6

A bilinear form on V is ***symmetric form*** if $\alpha(x, y) = \alpha(y, x)$ for all $x, y \in V$.

Definition 1.7

If $(x_1, ..., x_n)$ is a basis of V and α be a bilinear form, then the ***Gram matrix*** of α is the $n \times n$ matrix with $A_{ij} = \alpha(x_i, x_j)$. We write $A = [\alpha]_{x_1,...,x_n}$.

Proposition 1.8

$A \approx_{\mathbb{Q}} B$ iff there exists a bilinear form α such that $A = [\alpha]_{x_1,...,x_n}$ and $B = [\alpha]_{y_1,...,y_n}$ for some bases $x_1, ..., x_n$ and $y_1, ..., y_n$.

Proposition 1.9

$A \approx_{\mathbb{Q}} B$ iff there exists a bilinear form α such that $A = [\alpha]_{x_1,...,x_n}$ and $B = [\alpha]_{y_1,...,y_n}$ for some bases $x_1, ..., x_n$ and $y_1, ..., y_n$.

Proof. ($\Rightarrow$): Suppose $P^T AP = B$ with P invertible. Let $\alpha : \mathbb{Q}^n \times \mathbb{Q}^n \to \mathbb{Q}$ be the bilinear form given by $\alpha(x, y) = x^T Ay$. Let $e_1, ..., e_n$ be the standard basis, then $A = [\alpha]_{e_1,...,e_n}$. Since P is invertible, $Pe_1, ..., Pe_n$ is also a basis for $\mathbb{Q}^n$.

We claim $B = [\alpha]_{Pe_1,...,Pe_n}$. To see this, we note

$$\alpha(Pe_i, Pe_j) = (Pe_i)^T A(Pe_j) = e_i^T Be_j = B_{ij}$$

Thus we proved the desired claim.

($\Leftarrow$): Suppose $A = [\alpha]_{x_1,...,x_n}$ and $B = [\alpha]_{y_1,...,y_n}$ for some bilinear form. Thus we get change of basis matrix P so $y_i = \sum_{k=1}^n P_{ki} x_k$. But then we see

$$\begin{aligned} B_{ij} &= \alpha(y_i, y_j) \\ &= \sum_{k=1}^n \sum_{l=1}^n P_{ki} P_{lj} \alpha(x_k, x_l) \\ &= \sum_{k=1}^n \sum_{l=1}^n P_{ki} P_{lj} A_{kl} \\ &= \sum_{k=1}^n \sum_{l=1}^n (P^T)_{ik} A_{kl} P_{lj} \\ &= (P^T A P)_{ij} \end{aligned}$$

Proposition 1.10

The Gram matrix of α is symmetric iff α is a symmetric form.

Since the matrices we are interested in are symmetric, we will only consider symmetric forms.

Theorem 1.11: Diagonal Theorem

Let $\alpha : V \times V \to \mathbb{Q}$ be symmetric. Then there exists a basis $x_1, \ldots, x_n$ for V such that $[\alpha]_{x_1,\ldots,x_n}$ is diagonal.

We note, if $\alpha : V \times V \to \mathbb{Q}$ is symmetric form and $W \subseteq V$ a subspace, then we get a symmetric form $\alpha_W : W \times W \to \mathbb{Q}$ by restricting the domain of α.

Proof. By induction on $\dim V$.

If $\dim V = 1$ then any basis diagonalizes α. Assume $\dim V = n$ and the result holds for $\dim < n$.

Case 1: Suppose $\alpha(x, x) = 0$ for all $x \in V$. Then

$$\alpha(x, y) = \frac{1}{2} \cdot (\alpha(x + y, x + y) - \alpha(x, x) - \alpha(y, y)) = 0$$

for all $x, y \in V$. Thus for any basis $x_1, \ldots, x_n$ for V, $[\alpha]_{x_1,\ldots,x_n} = 0$ is the zero matrix.

Case 2: If $\alpha(x, x) \neq 0$ for some $x \in V$. Consider $W = \{w \in V : \alpha(x, w) = 0\} = \ker(\alpha(x, \cdot))$. We see $\alpha(x, \cdot)$ is a rank 1 linear map (rank ≤ 1 since $\dim \mathbb{Q} = 1$, rank > 0 since $x \notin \ker(\alpha(x, \cdot))$). Thus $\dim W = n - 1$. By induction hypothesis we can find basis $y_1, \ldots, y_{n-1}$ so $[\alpha_W]_{y_1,\ldots,y_{n-1}}$ is diagonal. Since $x \in W$, we see $x, y_1, \ldots, y_{n-1}$ is a basis for V.

We claim $[\alpha]_{x,y_1,\dots,y_{n-1}}$ is diagonal. Indeed, for all $j > 1$, $D_{1j} = D_{j1} = \alpha(x, y_{j-1}) = 0$ since $y_{j-1} \in W$. We also have

$$D_{ij} = D_{ji} = \alpha(y_{i-1}, y_{j-1}) = 0$$

for $i < j$.

Corollary 1.11.1

Every symmetric matrix is congruent to a diagonal matrix.

Definition 1.12

Let $\alpha : V \times V \to \mathbb{Q}$ be symmetric form. An invertible linear map $T : V \to V$ is an ***isometry*** of α if $\alpha(x, y) = \alpha(Tx, Ty)$ for all $x, y \in V$.

Theorem 1.13: Isometry Theorem

If $x, y \in V$ such that $\alpha(x, x) = \alpha(y, y) \neq 0$. Then there exists isometry $T : V \to V$ such that $Tx = y$.

Proof. Exercise

Theorem 1.14: Witt Cancellation

Let $A = \mathrm{Diag}(A_1, A_2), B = \mathrm{Diag}(B_1, B_2)$ be $n \times n$ symmetric matrices with diagonal block matrices. Suppose $A \approx_{\mathbb{Q}} B$ and $A_1 \approx_{\mathbb{Q}} B_1$ and A_1, B_1 are invertible. Then $A_2 \approx_{\mathbb{Q}} B_2$.

Proof. By the diagonal theorem we can find D so $A_1 \approx_{\mathbb{Q}} B_1 \approx_{\mathbb{Q}} D$. Thus we see we get

$$\begin{bmatrix} D & 0 \\ 0 & A_2 \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix} \approx_{\mathbb{Q}} \begin{bmatrix} D & 0 \\ 0 & B_2 \end{bmatrix}$$

Thus it suffices to consider the following special case.

Special case: let $c \in \mathbb{Q}$, $c \neq 0$. If

$$\begin{bmatrix} c & 0 \\ 0 & A_2 \end{bmatrix} \approx \begin{bmatrix} c & 0 \\ 0 & B_2 \end{bmatrix}$$

then $A_2 \approx_{\mathbb{Q}} B_2$.

To prove this special case, let α be a symmetric form on vector space V on $\mathbb{Q}$ such that it has two bases $x, w_1, \dots, w_{n-1}$ and $y, z_1, \dots, z_{n-1}$ such that

$$[\alpha]_{x,w_1,\dots,w_{n-1}} = \begin{bmatrix} c & 0 \\ 0 & A_2 \end{bmatrix}$$

$$[\alpha]_{y,z_1,\dots,z_{n-1}} = \begin{bmatrix} c & 0 \\ 0 & B_2 \end{bmatrix}$$

Note that $\alpha(x,x) = \alpha(y,y) \neq 0$. By t he isometry theorem we can find an isometry $T : V \to V$ such that $Tx = y$.

Let $W = \{z \in V : \alpha(y,z) = 0\} = \ker(\alpha(y,\cdot))$. As we saw in the diagonal theorem, $\dim W = n-1$.

We claim $z_1, \dots, z_{n-1}$ is a basis for W. Indeed, we have

$$\alpha(y, z_i) = \begin{bmatrix} c & 0 \\ 0 & B_2 \end{bmatrix}_{1,i+1} = 0$$

and hence $z_i \in W$. Furthermore, $z_1, \dots, z_{n-1}$ are linearly independent. Finally, it has the right size, hence it must be a basis as desired. This concludes the claim.

Similarly, we have $Tw_1, \dots, Tw_{n-1}$ is also a basis for W. Indeed, $\alpha(y, Tw_i) = \alpha(Tx, Tw_i) = \alpha(x, w_i) = 0$.

Finally, we see $B_2 = [\alpha|_W]_{z_1,\dots,z_{n-1}}$ and $A_2 = [\alpha|_W]_{Tw_1,\dots,Tw_{n-1}}$. Hence they are congruent as desired.

Now that we have a cancellation theorem we need something to cancel.

Theorem 1.15

For every positive integer n, $\mathrm{Id}_4 \approx_{\mathbb{Q}} n\,\mathrm{Id}_4$.

To prove this, we need more algebra.

First, we consider new ways to define complex numbers. In particular, complex numbers can be thought as 2×2 real matrices of the form

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

Then:

1. The set of such matrices is closed under $+, -, \cdot$ and inverse.

2. This $\mathbb{R}$-algebra is isomorphic to $\mathbb{C}$ under

$$a + bi \longleftrightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

In particular, we define the quaternion in a similar manner.

Definition 1.16

A ***(matrix) quaternion*** is a 4×4 matrix of the form

$$A = \begin{bmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{bmatrix}$$

Definition 1.17

The ***modulus*** of a quaternion given by a, b, c, d is defined as $|A| := \sqrt{a^2 + b^2 + c^2 + d^2}$.

We use $\mathbb{H}$ to denote the set of all quaternions.

Proposition 1.18

$\mathbb{H}$ is a $\mathbb{R}$-vector space. Moreover, let $A, B \in \mathbb{H}$.

1. $AB \in \mathbb{H}$
2. $A^T \in \mathbb{H}$
3. *If $A \neq 0$ then A is invertible and $A^{-1} \in \mathbb{H}$*
4. *In particular, $A^T = A = AA^T = |A|^2 I_4$ if $A \neq 0$. Hence $A^{-1} = \frac{1}{|A|^2} A^T$.*
5. $|AB| = |A| \cdot |B|$
6. *$|A| = 0$ iff $A = 0$.*

Well, however, we need to note, $AB \neq BA$ in general.

Definition 1.19

We say $A \in \mathbb{H}$ is called ***Hurwitz quaternion*** if either:

1. $A_{ij} \in \mathbb{Z}$ for all i, j, or
2. $A_{ij} \in \mathbb{Z}[\frac{1}{2}]$ for all i, j (note $\mathbb{Z}[\frac{1}{2}] = \mathbb{Z} + \frac{1}{2} = \{a + \frac{1}{2} : a \in \mathbb{Z}\}$).

This above condition for Hurwitz quaternion is the same as $2A$ has all integer entries with the same parity.

We use $\mathbb{A}$ to denote the set of all Hurwitz quaternions.

Proposition 1.20

If $A, B \in \mathbb{A}$, then:

1. $A + B \in \mathbb{A}$.
2. $mA \in \mathbb{A}$ *for all* $m \in \mathbb{Z}$.
3. $A^T \in \mathbb{A}$.
4. $AB \in \mathbb{A}$.
5. *If* $A^{-1} \in \mathbb{A}$ *then* $|A| = 1$.
6. $|A|^2 \in \mathbb{Z}_{\geq 0}$ *(i.e.* $a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}$*).*
7. *If* $X \in \mathbb{H}$*, then there exists* $[X] \in \mathbb{A}$ *such that* $|X - [X]| < 1$.

We will prove we can find $P \in \mathbb{A}$ such that $P^T I_4 P = nI_4$.

To prove $P^T I_4 P = nI_4$, we use extended Euclidean algorithm for integers.

To recall that, we do an example. Suppose we want to compute $\gcd(81, 30)$, we get

$$21 = 81 - 2 \cdot 30$$

$$9 = 30 - 21$$

$$3 = 21 - 2 \cdot 9$$

and

$$0 = 9 - 3 \cdot 3$$

This gives a sequence $81, 30, 21, 9, 3, 0$ and hence the gcd is the last non-zero entory, i.e. 3. This is one application of Euclidean algorithm.

We can also use Euclidean algorithm to express the gcd in terms of two original numbers, i.e. we get $3 = 3 \cdot 81 - 8 \cdot 30$.

Lemma 1.21: Left GCD for Hurwitz Quaternions

Let $A_0, A_1 \in \mathbb{A}$ *and* $A_0 \neq 0$. *Then there exist a Hurwitz quaternion* $G \in \mathbb{A}$ *such that:*

1. $G^{-1}A_0 \in \mathbb{A}$, $G^{-1}A_1 \in \mathbb{A}$
2. $G = A_0 X_0 + A_1 X_1$ *for some* $X_0, X_1 \in \mathbb{A}$.

In this case, G *is said to be a left-GCD of* A_0 *and* A_1.

Proof. Construct a sequence $A_0, A_1, A_2, \ldots$ as follows: for $k \geq 0$, let

$$A_{k+2} := A_k - A_{k+1}[A_{k+1}^{-1} A_k]$$

where $[A_{k+1}^{-1} A_k]$ is rounding opeartion. This is the same as

$$A_{k+2} = A_{k+1}(A_{k+1}^{-1} A_k - [A_{k+1}^{-1} A_k])$$

We can do this as long as $A_{k+1} \neq 0$. This is clearly a Hurwitz quaternion and hence all A_k are Hurwitz quaternions. The second equation about A_{k+2} shows $|A_{k+1}| < |A_k|$.

Since this is strictly decreasing, we see this sequence must stop at one point. Then, the proof is the same as the proof of Euclidean algorithm for integers.

Lemma 1.22

For every prime p, there exists integer m, $1 \le m \le p$ and integers x, y such that

$$1 + x^2 + y^2 = mp$$

Proof. Assume p is odd. Consider

$$0^2, 1^2, \dots, (\frac{p-1}{2})^2$$

and

$$-1-0^2, -1-1^2, \dots, -1-(\frac{p-1}{2})^2$$

There are $p+1$ numbers between these two sequences. Hence two of these numbers must be equal mod p. In particular, these two numbers cannot come from the same sequence. Indeed, they cannot both come from the first sequence because $x^2 \equiv y^2 \pmod p$ and hence $x \equiv y \pmod p$ or $x \equiv -y \pmod p$. Similarly they cannot both come from the second. Hence, we get $x^2 \equiv -1 - y^2 \pmod p$. But note $0 \le x \le \frac{p-1}{2}$ and $0 \le y \le \frac{p-1}{2}$, hence we conclude

$$1 + x^2 + y^2 < p^2 \Rightarrow 1 + x^2 + y^2 = mp$$

with $m < p$.

Lemma 1.23

For every prime p, there exists a Hurwitz quaternion $G_r \in \mathbb{A}$ such that $|G_p| = \sqrt{p}$.

Proof. Let x, y, m be as previous lemma. Let

$$A_0 = \begin{bmatrix} 1 & \dots \\ x & \dots \\ y & \dots \\ 0 & \end{bmatrix} \in \mathbb{A}$$

and let $A_1 = pI_4 \in \mathbb{A}$. Then $|A_0| = \sqrt{1 + x^2 + y^2} = \sqrt{mp}$ with $1 \le m \le p$ and $|A_1| = p = \sqrt{p \cdot p}$. If $p = 2$ then $m = 1$ so $G_p = A_0$. If p is odd, then let G_p be the left GCD of A_0 and A_1.

Since $G_p \in \mathbb{A}$, we get $G_p^{-1}A_i \in \mathbb{A}$ for $i = 0, 1$ and hence

$$|G_p|^2 \cdot |G_p^{-1}A_0|^2 = |A_0|^2 = mp$$

This means $|G_p|^2 \mid mp$. Moreover

$$|G_p|^2 \cdot |G_p^{-1}A_1|^2 = |A_1|^2 = p^2$$

and so $|G_p|^2$ divides p^2.

Since $|G_p|^2 \in \mathbb{Z}$ we deduce that $|G_p|^2 = 1$ or $|G_p|^2 = p$. To rule out the first case, we see $|G_p|^2 = 1$ means $|G_p| = 1$ and hence $G_p^{-1} \in \mathbb{A}$ by properties of Hurwitz quaternions. Write $G_p = A_0X_1 + A_1 + X_1$ with $X_i \in \mathbb{A}$. Then we get

$$\begin{aligned}
A_0^T &= A_0^T G_p G_p^{-1} \\
&= A_0^T (A_0 X_0 + A_1 X_1) G_p^{-1} \\
&= A_0^T A_0 X_0 G_p^{-1} + A_0^T A_1 X_1 G_p^{-1} \\
&= mpX_0 G_p^{-1} + pA_0^T X_1 G_p^{-1} \\
&= p \cdot (\ldots)
\end{aligned}$$

which implies $A_0^T \in p\mathbb{A}$, which is a contradiction as A_0^T contains x, y and it is not a multiple of p. Hence $|G_p|^2 = p$ as desired.

Theorem 1.24

If n is a positive integer, then $I_4 \approx_{\mathbb{Q}} nI_4$.

Proof. Write $n = p_1 \ldots p_l$ with p_i prime. Let $p = G_{p_1} \ldots G_{p_l} \in \mathbb{A}$, then $|p| = \prod |G_{p_i}| = \sqrt{n}$. Hence $P^T I_4 P = |P|^2 I_4 = nI_4$ as desired.