MA4006-1. Combinatoria 2014.
Profesor: José Soto.

Advertencia: Este apunte es un borrador de las clases de MA4006 Combinatoria realizadas el año 2014. Puede contener errores involuntarios, por favor informar de cualquier error de texto y/o formato al correo jsoto@dim.uchile.cl

V. Hipergrafos y diseños.

Una **estructura de incidencia** o **diseño** es un triple $S = (\mathcal{V}, \mathcal{E}, I)$, donde

1. $\mathcal{V}$ es un conjunto cuyos elementos son llamados puntos o vértices.
2. $\mathcal{E}$ es un conjunto cuyos elementos son llamados bloques o aristas (hiperaristas).
3. I es una relación de incidencia entre V y E, es decir $I \subseteq \mathcal{V} \times \mathcal{E}$. Los elementos de I son normalmente llamados banderas. Podemos ver I también como una **matriz de incidencia** donde $I(v, B) = 1$ si $(v, B) \in I$.

Si $(v, B) \in I$ decimos que el punto v y el bloque B son incidentes. En general, permitimos que dos bloques distintos B_1 y B_2 sean incidentes a los mismos puntos. Cuando esto no pasa decimos que el diseño es **simple**. El **soporte** de un bloque B es el conjunto de puntos incidentes a B (lo denotamos como $\text{sop}(B)$).

Un diseño simple también se conoce como **"hipergrafo"**. En dicho caso, se suelen llamar a los bloques "aristas" y a los puntos "vértices". Además, interpretamos los bloques de $\mathcal{E}$ como subconjuntos de $\mathcal{V}$ (aquellos puntos incidentes al bloque). En otras palabras, un hipergrafo $H = (\mathcal{V}, \mathcal{E})$ es un par tal que $\mathcal{E} \subseteq 2^{\mathcal{V}}$.

Sea $S = (\mathcal{V}, \mathcal{E}, I)$ un diseño.

- El **grado** de un punto $v \in \mathcal{V}$, denotado $\deg(v)$ es el número de bloques incidentes a él.
- El **tamaño** de un bloque $B \in \mathcal{E}$, denotado $s(B)$ (o simplemente $|B|$ en el caso de hipergrafos) es igual al número de puntos incidentes a él.
- Un diseño es k-**uniforme** si todos los bloques tienen tamaño k
- Un diseño es k-**regular** si todos los puntos tienen grado k.
- El **dual** de un diseño $S = (\mathcal{V}, \mathcal{E}, I)$ es el diseño $S^* = (\mathcal{E}, \mathcal{V}, I^*)$ donde $(v, B) \in I$ si y solo si $(B, v) \in I^*$.
  Los conceptos de grado y tamaño se dualizan. En particular, el dual de un diseño k-uniforme es k-regular, y viceversa.

Notemos que en un hipergrafo k-uniforme, $\mathcal{E} \subseteq \binom{\mathcal{V}}{k}$. Agreguemos algo de notación para hipergrafos.

- Un hipergrafo 2-uniforme se conoce como **grafo** (simple).
- Un diseño con $|B| \in \{1, 2\}$ se conoce como **multigrafo**.
- El **complemento** (estándar) de $H = (\mathcal{V}, \mathcal{E})$ es $(\mathcal{V}, 2^{\mathcal{V}} \setminus \mathcal{E})$.
- El **complemento** (uniforme) de un hipergrafo k-uniforme $H = (\mathcal{V}, \mathcal{E})$ es $(\mathcal{V}, \binom{\mathcal{V}}{k} \setminus \mathcal{E})$.
- Por conveniencia, llamaremos n al tamaño de $\mathcal{V}$ y m al tamaño de $\mathcal{E}$.

Diseños de líneas

Estamos interesados en estudiar diseños con algún tipo de estructura regular. El primer ejemplo que veremos son los llamados diseños de líneas.

[Def] En un **diseño de líneas** los bloques son llamados **líneas**. Cada linea contiene (es decir, es incidente a) al menos 2 puntos y cada par de puntos están en exactamente una linea. En particular, el diseño es simple.
Ejemplos: Aparte de los ejemplos triviales (un punto sin bloques, o 0 puntos) los siguientes son fáciles de ver:

1. Grafos completos $K_n = ([n], \binom{n}{2})$.

2. En general, hipergrafos completos k-uniformes: $K_n^{(k)} = ([n], \binom{n}{2})$.

3. Plano de Fano $([7], \{\{1,2,3\},\{3,4,5\},\{5,6,1\},\{1,7,4\},\{3,7,6\},\{5,7,2\},\{2,4,6\}\})$

Teorema 1 (Erdös, de Brujin)**.** *Si S es un diseño de líneas no trivial con $n \geq 2$ entonces $m = 1$ o $m \geq n$, y de tener igualdad se tiene que para cada par de líneas existe exactamente un punto incidente a ambos.*

Demostración. Como $n \geq 2$ hay al menos una linea. Supongamos que hay más de una. Si $x \notin L$ entonces $\deg(x) \geq |L|$ pues hay $|L|$ líneas distintas que unen a x a los puntos de L (de hecho, observamos que si existiera una linea L' disjunta a L que pasa por x entonces, $\deg(x) > |L|$). Supongamos que $m \leq n$. Entonces $m(n - |L|) \geq n(m - \deg(x))$ y luego,

$$1 = \sum_{x \in \mathcal{V}} \sum_{L \in \mathcal{E}, L \not\ni x} \frac{1}{n(m - \deg(x))} \geq \sum_{L \in \mathcal{E}} \sum_{x \notin \mathcal{V}} \frac{1}{n(m - \deg(x))} = 1.$$

Luego la desigualdad debe ser igualdad y de hecho, para todo $x \notin L$, $n(m - \deg(x)) = m(n - |L|)$, luego, $n \deg(x) = m|L|$ y como $m \leq n$, $|L| \leq \deg(x)$ se concluye que $m = n$ y $L = \deg(x)$. Usando la observación del principio de la demostración, notamos que no pueden haber dos líneas disjuntas. □

Ejemplo: Un **casi-lapiz** (o casi-haz) es un diseño de líneas con $m = n > 2$, $\mathcal{V} = [n]$, y cuyas líneas son $\{1, n\}, \{2, n\}, \ldots, \{n-1, n\}, [n-1]$.

t-Diseños

Definiciones:

- Decimos que dos diseños H y H' son **isomorfos** si existen funciones $f\colon \mathcal{V}(H) \to \mathcal{V}(H')$, $g\colon \mathcal{E}(H) \to \mathcal{E}(H')$ biyectivas tal que $\operatorname{sop}(g(B)) = f(\operatorname{sop} B)$. Alternativamente, dos diseños son isomorfos si la matriz de incidencia de una se puede obtener de la otra permutando filas y coumnas. En el caso de hipergrafos, la funcion g esta determinada, $g(B) = f(B)$. Luego basta mostrar $f\colon \mathcal{V}(H) \to \mathcal{V}(H')$ biyectiva tal que $B \in E(H)$ si y solo si $f(B) \in E(H')$.

- Sea $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ un hipergrafo (o un diseño) y $X \subseteq \mathcal{V}$, el **grado** de X, $\deg(X)$ es el número de bloques que contienen a X como subconjunto (que son incidentes a los puntos de X). En particular, $\forall v \in \mathcal{V}, \deg(\{v\}) = \deg(v)$ y $\deg(\emptyset) = m = |\mathcal{E}|$.

- Un diseño se dice (t, λ)-**balanceado** si $\forall X \in \binom{\mathcal{V}}{t}$, $\deg(X) = \lambda$ (notar que $(1, \lambda)$-balanceado es lo mismo que λ-regular).

- Un t-**diseño**, es un diseño uniforme, (t, λ)-balanceado para algún λ. Más específicamente un t-diseño se denota $S_\lambda(t, k, n)$ si tiene n puntos, k-uniformes y (t, λ)-balanceado ($\lambda \geq 1$ se conoce como el índice del diseño, notar que $t \leq k \leq n$).

- Un t-diseño se llama trivial si $t = k$ o $k = n$. Cuando $k = n$, tenemos que todos los bloques contienen a todos los puntos, luego $\lambda = m$. Por otro lado si $t = k$, entonces todo conjunto de t puntos está contenido en λ bloques "iguales" (incidentes a los mismos puntos). Es decir el diseño no es más que λ copias de $([n], \binom{n}{t})$. Por estas razones, usualmente se pide que $t < k < n$.

- En este curso nos preocuparemos solo de diseños simples o hipergrafos (pero las definiciones se extienden a casos generales).

- Un **sistema de Steiner** es un t-diseño con índice 1, en ese caso se denota $S(t, k, n)$ (esto es un hipergrafo k-uniforme, donde cada conjunto de t puntos está contenido en 1 bloque).

- Los 2-diseños, i.e. $S_\lambda(2, k, n)$ tambien se conocen como BIBD (balanced incomplete block design).

- Los t-diseños con $n = m$ se llaman simétricos (igual numero de puntos que de bloques).

Ejemplos

1. Grafos λ-regulares son $S_\lambda(1,2,n)$.
2. El plano de Fano es un $S(2,3,7)$ (notar que es un BIBD)
3. Sea $\mathbb{F}_p$ el cuerpo de orden p para p primo. Considere el hipergrafo H $\mathcal{V} = \mathbb{F}_p^4 \setminus \{\vec{0}\}$ y $\mathcal{E} = \{\{x,y,z\}\colon x+y+z=\vec{0}\}$. Cada par de elementos $x \neq y$ de $\mathcal{V}$ determina un único tercer elemento $z = -x-y = x+y$ tal que $\{x,y,z\}$ es un bloque (Notar que $z \neq x$ (y de y) pues si $z = x$ tendriamos $\vec{0} = x+y+x = y$). Luego, H tiene 15 puntos, es 3-uniforme y $(2,1)$-regular. Es decir, es un $S(2,3,15)$.
4. Sea ahora $\mathcal{V} = \mathbb{F}_p^4$, $\mathcal{E} = \{\{w,x,y,z\}\colon w+x+y+z=\vec{0}\}$. Nuevamente, si w,x,y son puntos distintos, existe un único z distinto a ellos ($z = z+x+y$ implica que $x=y$) tal que $\{w,x,y,z\}$ es un bloque. Luego H es un $S(3,4,16)$.

A continuación veremos varios teoremas concernientes a relaciones entre los parámetros de un t-diseño. Notamos que los teoremas 2, 3 y 4 son generalizados por el teorema 5.

Teorema 2. *El número de bloques de un $S_\lambda(t,k,n)$ es*

$$m = \lambda\binom{n}{t}/\binom{k}{t} = \lambda\binom{n}{k}/\binom{n-t}{k-t}.$$

Demostración. Cree el grafo bipartito G con vértices en un lado $L = \binom{n}{t}$ y del otro $R = \mathcal{E}$, los bloques de H. Un par (T,B) es una arista del grafo si $T \subseteq B$. Notar que todos los vértices de L tienen grado λ, luego el número de aristas es $|L|\lambda = \lambda\binom{n}{t}$. Por otro lado todos los vértices de R tienen grado $\binom{k}{t}$, es decir el número de aristas es $m\binom{k}{t}$. □

Teorema 3. *Considere un $S_\lambda(t,k,n)$ y sea $0 \leq i \leq t$. Para todo conjunto $I \in \binom{n}{i}$,*

$$\deg(I) = \lambda\binom{n-i}{t-i}/\binom{k-i}{t-i} = \lambda\binom{n-i}{k-i}/\binom{n-t}{k-t}$$

Demostración. Cree el grafo bipartito G' con vértices en un lado L los conjuntos de t puntos que contienen a I y del otro $R = \mathcal{E}$, los bloques de H. Un par (T,B) es una arista del grafo si $T \subseteq B$. Notar que G' es subgrafo inducido de G. El grado de los vertices de L es λ. Luego el n[umero de aristas es $|L|\lambda = \lambda\binom{n-i}{t-i}$. Por otro lado los vertices de R tienen grado $\binom{k-i}{t-i}$, luego el numero de aristas es $\deg(I)\binom{k-i}{t-i}$ □

En particular, todos los t-diseños también son i-diseños ($S_{\deg(I)}(i,k,n)$) y son r-regulares donde $r = \lambda\binom{n-1}{t-1}/\binom{k-1}{t-1}$.
La existencia de diseños $S_\lambda(t,k,n)$ para distintos parámetros es un tema central de esta área. En particular sabemos:

Corolario 1. *Si existe $S_\lambda(t,k,n)$ entonces para todo $0 \leq i \leq t$,*

$$\binom{n-i}{t-i}/\binom{k-i}{t-i} = \frac{(n-i)!(t-i)!(k-t)!}{(t-i)!(n-t)!(k-i)!} = \frac{(n-i)!(k-t)!}{(k-i)!(n-t)!} = \frac{(n-i)(n-(i+1))\dots(n-(t-1))}{(k-i)(k-(i+1))\dots(k-(t-1))}$$

son numeros naturales.

De aquí se deduce, por ejemplo que los n para los cuales hay un $S(2,4,n)$, deben satisfacer $(n-1)/3$ y $n(n-1)/12$ son naturales, es decir, $n = 1$ modulo 3. Lo que implica que n es 1 o 4 modulo 12 (no puede ser 7 o 11).

Corolario 2. *Para 2-diseños, $r(k-1) = \lambda(n-1)$ y $mk(k-1) = \lambda n(n-1)$ o sea $mk = nr$.*

Volvamos un poco a los diseños de líneas simétricos (i.e. $n = m$). Los diseños de líneas son $(2,1)$-balanceados (cada par de puntos está en 1 linea), el tamaño de cada bloque es al menos 2. Sea D uno de estos diseños.

Ejercicio 1. Probar que si D es un diseño de líneas no uniforme, entonces D es un casi-lapiz.

En el caso uniforme, tenemos que D es un 2-diseño simétrico con indice $\lambda = 1$.

[Def]**Plano Proyectivo:** Un plano proyectivo es un 2-diseño simétrico con $\lambda = 1$.
[Def]**Diseño Proyectivo:** Un diseño proyectivo es un 2-diseño simétrico (a veces se denotan SBIBD).

Normalmente llamamos a $q = k - \lambda$ el**orden** del diseño proyectivo. En todo diseño proyectivo, $r = k$ y $k(k-1) = \lambda(n-1)$. Es decir, los diseños proyectivos son los

$$S_\lambda(2, k, 1 + (k(k-1))/\lambda) = S_\lambda(2, q + \lambda, 1 + (q + \lambda)(q + \lambda - 1)/\lambda).$$

Para el caso de planos proyectivos, se tiene un

$$S(2, k, k^2 - k + 1) = S(2, q + 1, q^2 + q + 2).$$

Planos proyectivos $PG(2, q)$

Sea q una potencia de primo de modo que el cuerpo $\mathbb{F}_q$ exista. Consideremos el espacio vectorial $\mathbb{F}_q^3$. ¿Cuántos subespacios vectoriales de dimensión 1 tiene $\mathbb{F}_q^3$?
Para ver esto, notemos que cada espacio vectorial de dimensión 1 tiene $q - 1$ vectores no nulos (que son paralelos). Como hay $q^3 - 1$ vectores no nulos se tiene que hay $(q^3 - 1)/(q - 1) = q^2 + q + 1$ espacios de dimensión 1. Tomemos estos como nuestros "puntos". Como bloques tomemos los espacios bidimensionales y la relacion de incidencia va por inclusion. El numero de espacios bidimensionales es el mismo (pues cada espacio bidimensional es el ortogonal de un espacio unidimensional). Luego el diseño es simétrico. Además es $(2, 1)$-balanceado (cada par de puntos está en exactamente un bloque). Por lo que se deduce que es un plano proyectivo $S(2, q+1, q^2+q+1)$ (el hecho que $k = q+1$ se puede sacar directamente o usando la ecuación $k(k-1) = n$). Este plano proyectivo usualmente se denota como $PG(2, q)$ (geometria proyectiva de dimension 2 y orden q).

Como ejemplo, el plano de Fano es isomorfo a $PG(2, 2)$ (para $q = 2$, los espacios vectoriales de dimension 1 tienen 1 vector no nulo). Los siete vectores no nulos de $\mathbb{F}_2^3$ son los puntos.

De la construcción anterior sabemos entonces que para toda potencia de primo q existe un plano proyectivo de orden q. Además, para ciertos q potencias de primo (ej: $q = 9$) se conocen planos proyectivos distintos a $PG(2, q)$. Nadie sabe si existen planos proyectivos con q no potencia de primo (no se descarta la posibilidad de ello).
Una definicion alternativa de plano proyectivo es la siguiente.

[Def]**Plano proyectivo** (alternativa): Un plano proyectivo es un hipergrafo que satisface

1. Cada par de puntos están en una única línea (dos puntos definen una linea).
2. Cada par de líneas intersectan en un único punto (no hay líneas paralelas).
3. Existe un conjunto de 4 puntos tales que no hay 3 en la misma línea (evita trivialidades).

Ejercicio 2. Probar que ambas definiciones de planos proyectivos son equivalentes.

Comentario: Para ganar un poco de intuición sobre los planos proyectivos, es conveniente mirar el plano proyectivo real $PG(2, \mathbb{R})$ que se obtiene reemplazando el cuerpo $\mathbb{F}_q$ por $\mathbb{R}$. Ya que tenemos un "punto" por cada dirección (vectores no paralelos) de $\mathbb{R}^3$, podemos pensar que en verdad nuestros puntos tienen todos norma 1, es decir es la bola de centro 0 y radio 1 en $\mathbb{R}^3$. Como dos puntos antipodales son paralelos debemos identificarlos. La forma más natural de hacer esto es mantener un hemisferio cerrado de la esfera e identificar puntos opuestos en el ecuador. Luego, los puntos del plano proyectivo son puntos del hemisferio y las líneas son los "círculos mayores". Si aplanamos el hemisferio (por ejemplo, ubicando el hemisferio sobre un plano y proyectando cada punto x de el al punto x' del plano obtenido al proyectar x desde el centro mediante una recta), tenemos realmente un plano con un punto en infinito agregado para cada dirección (y una "linea"que pasa por todos los puntos en infinito). El nombre de "plano proyectivo" viene esencialmente de su interpretación artística: Si vemos dos líneas paralelas de acuerdo a la geometría habitual (por ejemplo las líneas de un riel de ferrocarril) de frente veremos que ambas líneas parecen converger al mismo punto en el horizonte, por ello decimos que se intersectan en infinto. El "horizonte" corresponde a la linea que pasa por los puntos al infinito.

Operaciones en diseños

Sea $D = (\mathcal{V}, \mathcal{E}, I)$ un diseño y $X \subseteq \mathcal{V}$. Definimos

1. **Borrado de X**:
$$D \setminus X = (\mathcal{V} \setminus X, \{B \in \mathcal{E} \colon \operatorname{sop}(B) \in \mathcal{E} \setminus X\})$$
notar que si D es hipergrafo,
$$D \setminus X = (\mathcal{V} \setminus X, \{B \in \mathcal{E} \colon X \cap B = \emptyset\}).$$

2. **Contracción de X** (Es borrar X y reducir las aristas incidentes):
$$D/X = (\mathcal{V} \setminus X, \{B_X \colon B \in \mathcal{E}\}),$$
donde B_X es un bloque que es incidente a todos los puntos de $\operatorname{sop}(B) \setminus X$.
Notar que si aplicamos la contracción a hipergrafos, podemos obtener diseños que no son hipergrafos, pues el resultado puede contener aristas múltiples (es decir, bloques incidentes a los mismos puntos).
Definimos entonces la contracción de vértices en hipergrafos como aquel hipergrafo que se obtienen primero aplicando la operación como diseño y luego borrando bloques múltiples (dejando un representante por clase de incidencia) y luego borrando aristas vacias. Es decir,
$$D/X = (\mathcal{V} \setminus X, \{B \setminus X \colon B \in \mathcal{E}, X \subsetneq B\}).$$

Ejercicio 3. Demostrar que la derivación y el borrado de vértices de diseños (resp. de hipergrafos) conmutan. Es decir si I y J son conjuntos disjuntos de vértices entonces $(D/I) \setminus J = (D \setminus J)/I$, $(D/J)/I = (D/I)/J$, $(D \setminus J) \setminus I = (D \setminus I) \setminus J$.

Definiremos 4 diseños asociados a un hipergrafo: Sea $H = (\mathcal{V}, \mathcal{E})$, $I \subseteq \mathcal{V}$.

1. **Diseño residual de H en I**
$$Res(H, I) = (\mathcal{V} \setminus I, \{B \colon B \cap I = \emptyset\}) = H \setminus I.$$

2. **Diseño derivado de H en I**
$$Der(H, I) = (\mathcal{V} \setminus I, \{B \setminus I \colon I \subseteq B\} \setminus \{\emptyset\})$$
(Es igual al hipergrafo obtenido al primero borrar las aristas que no contienen a I, y luego contraer I.

3. **Diseño residual interno de H en I**
$$ResInt(H, I) = (\mathcal{V} \setminus I, \{B \setminus I \colon B \in \mathcal{E}\} \setminus \{\emptyset\})$$

4. **Diseño derivado interno de H en I**
$$DerInt(H, I) = (I, \{B \cap I \colon B \in \mathcal{E}\} \setminus \{\emptyset\})$$

Como ejemplo, para el sistema de Steiner $S(3, 4, 16)$ dado por $H = (\mathbb{F}_p^4, \{\{w, x, y, z\} \colon w + x + y + z = \vec{0}\})$, su derivado en $\vec{0}$ es el $S(2, 3, 15)$ dado por $Der(H, \{\vec{0}\}) = (\mathbb{F}_p^4 \setminus \{\vec{0}\}, \{\{x, y, z\} \colon x + y + z = \vec{0}\})$.

Corolario 3. *Sea H es un $S_\lambda(t, k, n)$ (no trivial). Entonces $Der(H, I)$ es un $S_\lambda(t - i, k - i, n - i)$ (no trivial).*

Demostración. Basta ver que $|\mathcal{V} \setminus I| = n - i$, que todo bloque tiene tamaño $k - i$ y que para todo $X \subseteq \mathcal{V} \setminus I$ con $|X| = t - i$,
$$\deg_{H_I}(X) = |\{B \setminus I \colon I \subseteq B \in \mathcal{E}, X \subseteq B \setminus I\}| = |\{B \in \mathcal{E} \colon X \cup I \subseteq B\}| = \deg_H(I \cup X) = \lambda. \quad \square$$

Teorema 4. *Sea $0 \leq j \leq t$ y $J \subseteq \binom{\mathcal{V}}{j}$ El número de bloques de un $S_\lambda(t, k, n)$ que **no** contienen a ningún punto de J es igual a*
$$\lambda \binom{n - j}{k} / \binom{n - t}{k - t}.$$

Demostración. Llamemos d_J a la cantidad buscada y usemos inclusión-exclusión. Usando que el grado de un conjunto de tamaño i es lambda $\binom{n-i}{t-i}/\binom{k-i}{t-i}$, se tiene

$$\begin{aligned}
d_J &= m - \sum_{I\colon \emptyset \neq I \subseteq J} (-1)^{|I|+1} |\{B \in \mathcal{E}\colon I \subseteq B\}| \\
&= \sum_{i=0}^{j} (-1)^i \binom{j}{i} \lambda \binom{n-i}{t-i} / \binom{k-i}{t-i} \\
&= \frac{\lambda}{\binom{n-t}{k-t}} \sum_{i\geq 0} (-1)^i \binom{j}{i} \binom{n-i}{n-k} \\
&= \frac{\lambda}{\binom{n-t}{k-t}} [x^n] \left(\left(\sum_{i\geq 0} (-1)^i \binom{j}{i} x^i \right) \left(\sum_{i\geq 0} \binom{i}{n-k} x^i \right) \right) \\
&= \frac{\lambda}{\binom{n-t}{k-t}} [x^n] \left((1-x)^j \frac{x^{n-k}}{(1-x)^{n-k+1}} \right) \\
&= \frac{\lambda}{\binom{n-t}{k-t}} [x^n] \left(\frac{x^{n-k}}{(1-x)^{n-k-j+1}} \right) \\
&= \frac{\lambda}{\binom{n-t}{k-t}} [x^n] \sum_{i\geq k} \binom{i}{n-k-j} x^{i+j} \\
&= \frac{\lambda}{\binom{n-t}{k-t}} \binom{n-j}{n-k-j}.
\end{aligned}$$

□

La demostración anterior se puede hacer más corta. De la segunda línea de la demostración anterior sabemos que d_J sólo depende de la cardinalidad de J y no de sus puntos. Llamemos d_j a este número en comun y creemos un grafo bipartito G con bipartición $(\binom{\mathcal{V}}{j}, \mathcal{E})$ y aristas (T, B) con $T \cap B = \emptyset$. Tenemos que el número de aristas de este grafo es $d_j \binom{n}{j} = m\binom{n-k}{j}$. Es decir

$$d_j = m\binom{n-k}{j} / \binom{n}{j} = \lambda \frac{\binom{n}{t}\binom{n-k}{j}}{\binom{k}{t}\binom{n}{j}} = \lambda \binom{n-j}{k} / \binom{n-t}{k-t}.$$

Podemos extender el teorema anterior aún más.

Teorema 5. *Sean I y J dos subconjuntos disjuntos de $\mathcal{V}$ en un $S_\lambda(t,k,n)$, con $|I| = i, |J| = j, i+j \leq t$. Entonces el número de bloques que son incidentes a todos los puntos de I y a ningún punto de J son*

$$\lambda \binom{n-i-j}{k-i} / \binom{n-t}{k-t}.$$

Demostración. La cantidad buscada es exactamente el número de bloques que no tocan a J en el sistema derivado con respecto a I, que es un $S_\lambda(t-i, k-i, n-i)$. Usando el teorema anterior para estos parámetros se concluye. □

Corolario 4. *Sea H un $S_\lambda(t,k,n)$. Si $J \subseteq \mathcal{V}$, $|J| \leq t$ entonces el hipergrafo residual $Res(H,J)$ es un $S_\mu(t-j, k, n-j)$ con $\mu = \lambda\binom{n-j}{k} / \binom{k-t+j}{j}$.*

Demostración. Recordemos que $Res(H,J) = (\mathcal{V} \setminus J, \{B \in \mathcal{E}\colon B \cap J = \emptyset\})$. Tenemos que $|\mathcal{V} \setminus J| = n-j$, que todo bloque tiene tamaño k y que para todo $X \subseteq \mathcal{V} \setminus I$ con $|X| = t-j$,

$$\deg_{Res(H,J)}(X) = |\{B \in \mathcal{E}\colon X \subseteq B, B \cap J = \emptyset\}| = \lambda \binom{n-t}{k-t+j} / \binom{n-t}{k-t} = \lambda \binom{n-k}{j} / \binom{k-(t-j)}{j} \quad \square$$

Ejercicio 4. Pruebe que el complemento uniforme de un $S_\lambda(t,k,n)$ con $n \geq k+t$ es un t-diseño y encuentre sus parámetros.

Antes de proseguir mencionemos una extensión del corolario 1 de este apunte

Corolario 5. *Si existe un $S_\lambda(t,k,n)$ entonces para todo $0 \le i,j \le t$ tal que $i+j \le t$ los números*

$$\lambda \frac{\binom{n-i-j}{k-i}}{\binom{n-t}{k-t}} = \lambda(n-i)$$

son enteros positivos.

Más sobre 2-diseños

Volvamos nuevamente a 2-diseños $t=2$ (BIBD). Es decir, diseños para los cuales cada par de puntos pertenecen al mismo número de bloques. Ya vimos algunos 2-diseños simétricos con $\lambda = 1$ (planos proyectivos), veamos un ejemplo con $\lambda > 1$.

Ejemplo: Consideremos como puntos los casilleros de un tablero de 4×4 casilleros. Para cada casillero x, definimos un bloque B_x que contiene a todos los cuadrados que están en la misma fila o en la misma columna de x (exceptuando a x). Este diseño tiene $n=16$, $m=16$, $k=6$. Veamos que es $(2,\lambda)$-balanceado para algún λ.
Sean x, y dos casilleros.

1. Si x e y están en la misma fila (o columna), entonces los bloques que contienen a ambos son exactamente los bloques asociados a los otros dos casilleros de la fila (o columna).

2. Si x e y no están en la misma fila ni columna entonces los únicos bloques que contienen a ambos son los asociados al casillero determinados por la fila de x y la columna de y, y al casillero dado por la fila de y y la columna de x.

Luego, el diseño anterior es un $S_2(2,6,16)$ simétrico.

Una propiedad importante que cumplen los 2-diseños es la llamada desigualdad de Fisher que es una generalización de la desigualdad de Erdos y de Brujin (para diseños de líneas, donde $\lambda = 1$).

Teorema 6. *En todo 2-diseño, $m \ge n$.*

Demostración. La demostración es algebráica. Tomemos la matriz de incidencia M del diseño ($M \in \{0,1\}^{n\times m}$). Recordemos que $rn = km$ y que $\lambda(n-1) = r(k-1)$. Como $k < n$, se tiene que $\lambda = r(k-1)/(n-1) < r$. Como cada punto está en r bloques y cada bloque tiene k puntos, la matriz MM^T vale

$$MM^T(x,y) = \sum_{B\in\mathcal{E}} M(x,B)M(y,B) = \begin{cases} \lambda, & \text{si } x \neq y \\ r, & \text{si } x = y \end{cases}.$$

Es decir, si J es la matriz de unos e I es la diagonal,

$$MM^T = \lambda J + (r-\lambda)I$$

Como J tiene un valor propio igual a n, y el resto son 0, se concluye que la matriz MM^T tiene $n-1$ valores propios iguales a $r-\lambda$ y un valor propio igual a $(r-\lambda)+\lambda n = r+\lambda(n-1) = rk$. Luego MM^T tiene rango completo n. Con esto, M tiene rango n de lo cual $m \ge n$. □

De la desigualdad de Fisher y las igualdades $rn = km$, $\lambda(n-1) = r(k-1)$ se deducen otras. Por ejemplo

$$r = km/n \ge k$$
$$k(k-1)/\lambda \le n-1 \le r(r-1)/\lambda$$

con igualdad en el caso simétrico.
La desigualdad de Fisher nos permite obtener cotas para los parámetros de t-diseños con $t \ge 2$, usando diseños derivados. Por ejemplo, si H es un $S_\lambda(3,k,n)$ entonces su derivada en un punto cualquiera es un $S_\lambda(2,k-1,n-1)$. Recordando que el número de bloques del diseño derivado es $|\{B \in \mathcal{E} \colon B \supseteq \{*\}\}| = r$, se concluye que $r \ge n-1$.
Una de las preguntas fundamentales es la (no)-existencia de planos proyectivos de ciertas parametros.
Usando las ideas de la demostración anterior podemos probar el siguiente teorema.

Teorema 7 (Bruck-Rysen-Chowla)**.** *Supongamos que existe un 2-diseño simétrico* $S_\lambda(2,k,n)$

1. *Si* n *es par, entonces* $(k-\lambda)$ *es cuadrado perfecto.*
2. *Si* n *es impar, entonces la ecuacion* $z^2 = (k-\lambda)x^2 + (-1)^{(n-1)/2}\lambda w^2$ *tiene solucion* $(x,w,z) \in \mathbb{Z}^3$ *no trivial (distinta de* $(0,0,0)$*).*

Usando el siguiente lema de teoría de números (que no demostraremos) "Todo entero que se puede escribir como la suma de dos cuadrados racionales también se puede escribir como suma de cuadrados enteros", se concluye el siguiente corolario.

Corolario 6. *Si existe un plano proyectivo de orden* q *igual a 1 o 2 módulo 4, entonces* q *es la suma de dos cuadrados.*

Demostración. Notemos que $n = q^2+q+1 \equiv 3 \pmod 4$. El teorema BRC nos dice que existe (x,z,w) no trivial tal que $z^2 = qx^2 - w^2$, o bien $qx^2 = z^2 + w^2$. De aquí tenemos que $x \neq 0$ y luego $q = \frac{z^2}{x^2} + \frac{w^2}{x^2}$ es suma de dos cuadrados racionales. Por lo tanto, es suma de cuadrados enteros. □

El corolario anterior garantiza que no existen planos proyectivo de orden 6 o 14 por ejemplo.
Volvamos a la demostracion de BRC. Para esto necesitaremos dos resultados de Lagrange:

Lagrange: Todo número entero n se puede escribir como la suma de 4 cuadrados, es decir $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Más aún, si $q \neq 0$, la matriz

$$H(q) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & -a_4 & a_3 \\ -a_3 & a_4 & a_1 & -a_2 \\ -a_4 & -a_3 & a_2 & a_1 \end{pmatrix},$$

es invertible, $H(q)^{-1} = \frac{1}{q}H(q)^T$ y además, para todo $x = (x_1,x_2,x_3,x_4) \in \mathbb{Z}^4$, el vector $y = (y_1,y_2,y_3,y_4) = xH(q)$ satisface

$$q(x_1^2+x_2^2+x_3^2+x_4^2) = y_1^2+y_2^2+y_3^2+y_4^2.$$

Demostración de BCR. Como la matriz de incidencia M es cuadrada, tenemos que

$$\det(M)^2 = \det(MM^T) = (rk)(r-\lambda)^{n-1} = r^2(r-\lambda)^{n-1}.$$

Como $\det(M)$ es un entero, concluimos el caso n par. Veamos ahora el caso impar. En adelante sea $x = (x_1,\dots,x_n)$ una variable n-dimensional y llamemos a $q = r-\lambda$ el *orden* del diseño. Definamos para todo $1 \leq j \leq n$, las variables

$$L_j := L_j(x) = \sum_{i=1}^n M_{ij}x_i = (x^TM)_j$$

La ecuación $MM^T = \lambda J + qI$ implica que

$$\begin{aligned} L_1^2 + \cdots + L_n^2 &= \sum_{j=1}^n (x^TM)_j^2 = x^T(MM^T)x \\ &= \lambda x^TJx + qx^Tx \\ &= \lambda\left(\sum_{i=1}^n x_i\right)^2 + q\sum_{i=1}^n x_i^2. \end{aligned} \tag{1}$$

Veamos primero el caso $n \equiv 1 \pmod 4$. Separemos las variables en grupos de a 4 y definamos:

$$\begin{aligned} (y_1,y_2,y_3,y_4) &= (x_1,x_2,x_3,x_4)H(q) \\ (y_5,y_6,y_7,y_8) &= (x_5,x_6,x_7,x_8)H(q) \\ &\vdots \\ (y_{n-4},y_{n-3},y_{n-2},y_{n-1}) &= (x_{n-4},x_{n-3},x_{n-2},x_{n-1})H(q) \\ y_n &= x_n \\ u &= \sum_{i=1}^n x_n \end{aligned}$$

Luego,

$$\sum_{i=1}^{n} L_i^2 = \lambda u^2 + \sum_{i=1}^{n-1} y_i^2 + q y_n^2 \tag{2}$$

Recordemos ahora que la matriz $H(q)$ es invertible (y su inversa es racional), por lo tanto cada L_i es una función lineal a coeficientes racionales de los y_i, esto también es cierto para u. En otras palabras, la expresión (2) es una identidad que vale para todo vector $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$. Modifiquemos esta ecuación para obtener otras identidades. Escribamos $L_1 = \mu_1 y_1 + \sum_{i=2}^{n} \mu_i y_i$. Sea $y' = (y_2, \ldots, y_n) \in \mathbb{R}^n$ arbitrario.
Si $\mu_i \neq 1$ entonces definamos

$$y_1 = \frac{\sum_{i=2}^{n} \mu_i y_i}{(1-\mu_1)}.$$

De modo que $L_1 = \mu_1 y_1 + (1-\mu_1) y_1 = y_1$.
Si $\mu_1 = 1$, definamos

$$y_1 = -\frac{\sum_{i=2}^{n} \mu_i y_i}{2}$$

De modo que $L_1 = y_1 - 2y_1 = -y_1$. En cualquier caso, $L_1^2 = y_1^2$ y luego

$$\sum_{i=2}^{n} L_i^2 = \lambda u^2 + \sum_{i=2}^{n-1} y_i^2 + q y_n^2 \tag{3}$$

Es decir, tenemos la misma identidad pero con una variable menos (donde naturalmente reexpresamos los L_i y u como funciones lineales en $(y_2, \ldots, y_n)$ a coeficientes racionales). Repitiendo el mismo argumento $n-2$ veces tenemos que

$$L_n^2 = \lambda u^2 + q y_n^2$$

donde tanto L_n como w son múltiplos racionales de y_n. Supongamos que $L_n = a y_n$, y $u = b y_n$ con $a, b \in \mathbb{Q}$, y finalmente fijemos $y_n = 1$.

$$a^2 = \lambda b^2 + q.$$

Escribiendo $a = a_1/a_2$, $b = b_1/b_2$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, y $b_2, a_2 \neq 0$, tenemos que

$$(a_1 b_2)^2 = \lambda (b_1 a_2)^2 + q (a_2 b_2)^2.$$

Llamando $z = a_1 b_2$, $w = b_1 a_2$, $x = a_2 b_2$ concluimos que

$$z^2 = q x^2 + \lambda w^2 = q x^2 + (-1)^{(n-1)/2} w^2,$$

donde $x \neq 0$. Con esto finalizamos la demostración del caso $n \equiv 1 \pmod 4$.
Para el caso $n \equiv 3 \pmod 4$, primero agregamos una nueva variable x_{n+1} y sumamos $q x_{n+1}^2$ a ambos lados de (5). Para obtener,

$$\sum_{i=1}^{n} L_1^2 + q x_{n+1}^2 = \lambda \left(\sum_{i=1}^{n} x_i \right)^2 + q \sum_{i=1}^{n+1} x_i^2. \tag{4}$$

Creando variables y_1 hasta y_{n+1} ($n+1$ es múltiplo de 4 ahora), se obtiene la identidad

$$\sum_{i=1}^{n} L_1^2 + q x_{n+1}^2 = \lambda u^2 + q \sum_{i=1}^{n+1} y_i^2. \tag{5}$$

donde ahora consideramos x_{n+1} como función racional de los y_i.
Eliminando como antes, se obtiene que

$$q x_{n+1}^2 = \lambda u^2 + y_{n+1}^2$$

Tenemos ahora que $x_{n+1} = (a_1/a_2)y_{n+1}$, $u = (b_1/b_2)y_{n+1}$, con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $a_2, b_2 \neq 0$. Fijando $y_{n+1} = 1$ se tiene que:

$$q(a_1b_2)^2 = \lambda(b_1a_2)^2 + (a_2b_2)^2.$$

Llamando $z = a_2b_2 \neq 0$, $w = b_1a_2$ y $x = a_1b_2$ tenemos que

$$z^2 = qx^2 - w^2 = qx^2 + (-1)^{(n-1)/2}w^2.$$

□

Cuadrados Latinos

[Def]**Tablero:** Para nuestros propósitos llamaremos *tablero* de orden n a una matriz cuyas filas, columnas y símbolos están todos indexados por $\mathbb{Z}_n$.

[Def]**Cuadrado latino:** Un tablero A es un cuadrado latino de orden n si cada elemento de $\mathbb{Z}_n$ aparece una vez en cada fila y una vez en cada columna.

Ejemplo: $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ es un cuadrado latino de orden 3.

[Def]**Superposición de tableros:** Si A y B son tableros de orden n, definimos $A \star B$ como la matriz de orden n tal que $A \star B(i,j) = (A(i,j), B(i,j))$.

[Def]**Tableros ortogonales:** Dos tableros A y B de orden n se dicen ortogonales si todos los pares $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ aparecen como símbolos en $A \star B$.

Proposición 1. *Definimos los siguientes tableros de orden n*

$$R_n = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \dots & \vdots \\ n-1 & n-1 & \dots & n-1 \end{pmatrix}, S_n = R_n^T$$

Un tablero X de orden n es cuadrado latino si y solo si X es ortogonal a R_n y X es ortogonal a S_n.

Ejemplo:

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \star \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} (0,0) & (1,0) & (2,0) \\ (1,1) & (2,1) & (0,1) \\ (2,2) & (0,2) & (1,2) \end{pmatrix}.$$

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \star \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} (0,0) & (1,1) & (2,2) \\ (1,0) & (2,1) & (0,2) \\ (2,0) & (0,1) & (1,2) \end{pmatrix}.$$

Demostración. Directa. □

Problema de los oficiales de Euler. Euler propuso el siguiente problema. Pueden 36 (resp. n^2) oficiales de 6 (resp. n) regimientos con 6 (resp. n) rangos distintos ser puestos en una formación de 6 por 6 (resp. n por n) de modo que en cada fila y columna haya un oficial de cada rango y un oficial de cada regimiento.
Llamando a cada oficial (i,j) donde i es el rango (en $\mathbb{Z}_n$) y j el regimiento (en $\mathbb{Z}_n$), el problema se reduce a encontrar una matriz M que contenga a todos los pares ordenados (i,j) de modo que en cada fila y columna aparezca exactamente una vez cada símbolo i en la primera coordenada y lo mismo para la segunda coordenada.
En términos de nuestra notación anterior, el problema de Euler consiste en encontrar dos cuadrados latinos de orden n ortogonales. El problema específico de Euler es el caso $n = 6$, también conocido como el de los 36 oficiales.

Notemos que el problema tiene solución para $n = 1$ y para $n = 3$. Pero no lo tiene para $n = 2$ (pues los unicos cuadrados latinos que existen son $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y los pares $(A, A), (A, B), (B, B)$ no son ortogonales.

Obs: La superposición de dos cuadrados latinos ortogonales también se conoce como **cuadrado greco-latino**.

[Def] Un conjunto L de cuadrados latinos de orden n tales que cada par de ellos son ortogonales se dirán MOLS (Mutually orthogonal Latin Squares).

Veamos una manera de construir algunos conjuntos de MOLS.

Teorema 8. *Sea n entero positivo y r elemento invertible de $\mathbb{Z}_n$ (es decir, primo relativo con n). Sea $A := A^{(r,n)}$ el tablero tal que*

$$\forall i, j \in \mathbb{Z}_n, \quad a_{ij} = r \cdot i + j \pmod{n}.$$

Entonces la matriz A es un cuadrado latino.

Demostración. Notar que:

$$\begin{aligned} & a_{i,j} = a_{i,k} \\ \iff & r \cdot i + j \equiv_n r \cdot i + k \\ \iff & j \equiv_n k. \end{aligned}$$

y además, como r es invertible,

$$\begin{aligned} & a_{j,i} = a_{k,i} \\ \iff & r \cdot j + i \equiv_n r \cdot k + i \\ \iff & r \cdot j \equiv_n r \cdot k \\ \iff & j \equiv_n k. \end{aligned}$$

□

Teorema 9. *Sea p primo, entonces $\{A^{(1,p)}, \dots A^{(p-1,p)}\}$ es un MOLS de orden p y cardinalidad $p - 1$.*

Demostración. Ya sabemos que son cuadrados latinos. Veamos que $A = A^{(r,p)}$ y $B = A^{(s,p)}$ son ortogonales. En efecto, supongamos que algún par ordenado se repite en la yuxtaposición, digamos, que la fila i y columna j se repite con la fila k y la columna ℓ. Es decir tenemos la siguiente igualdad en $\mathbb{Z}_p^2$:

$$(r \cdot i + j, s \cdot i + j) = (r \cdot k + \ell, s \cdot k + \ell)$$

Reescribiendo tenemos que

$$r(i - k) = (\ell - j), \text{ y } s(i - k) = (\ell - j)$$

Si $i \neq k$, concluimos que $r = s$, cancelando $i - k$. Luego debemos tener que $i = k$. Pero entonces, deducimos de la primera ecuación que $j = \ell$. Es decir, la unica forma que dos posiciones tengan el mismo par ordenado es que las posiciones sean iguales. □

La construcción anterior se puede hacer también si en vez de indexar los símbolos y posiciones con el cuerpo $\mathbb{Z}_p$ lo indexamos con el cuerpo finito $\mathbb{F}_q$ donde q es una potencia de primo. En este caso tambien podemos construir un MOLS de orden q y cardinalidad $q - 1$.

Teorema 10. *Para todo q potencia de primo existe un conjunto de $q - 1$ MOLS de orden q.*

Como ejemplo veamos que pasa con el cuerpo de 4 elementos: $(0, 1, x, x + 1)$, donde $x + x = 0$, $x \cdot x = 1 + x$.
Las 3 matrices del MOLS son:

$$A^{(1,4)} = \begin{pmatrix} 0 & 1 & x & x+1 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \end{pmatrix}, A^{(x,4)} = \begin{pmatrix} 0 & 1 & x & x+1 \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \\ 1 & 0 & x+1 & x \end{pmatrix}, A^{(1+x,4)} = \begin{pmatrix} 0 & 1 & x & x+1 \\ x+1 & x & 1 & 0 \\ 1 & 0 & x+1 & x \\ x & 1+x & 0 & 1 \end{pmatrix},$$

Reetiquetando obtenemos 3 cuadrados latinos (tableros) mutualmente ortogonales de orden 4.

Notemos que siempre podemos reetiquetar los símbolos de un cuadrado latino mediante una permutación. Decimos que un cuadrado latino está en forma estándar, si su fila 0 es $(0, 1, 2, \ldots, n-1)$. Si quisieramos contar cuadrados latinos, bastaría con primero contar cuadrados latinos estándar (¿por qué?)

Dado un entero $n \geq 2$, llamemos $N(n)$ al número máximo de MOLS que podemos encontrar. Sabemos que $N(2) = 1$ y que si q es potencia de primo, $N(q) \geq q-1$. ¿Es posible encontrar un n tal que $N(n) \geq n$? La respuesta la da el siguiente teorema.

Teorema 11. *Para todo $n \geq 2$, $1 \leq N(n) \leq n-1$.*

Demostración. Supongamos que para cierto n, existen MOLS $A_1, \ldots, A_k$ con $k \geq n$. Observemos primero que podemos suponer que los cuadrados latinos están en forma estándar y eso no afecta la propiedad de MOLS. En particular, para cada par A_i, A_j, su superposición tiene fila 0: $(0,0), (1,1), \ldots, (n-1, n-1)$.
Notar que $A_i(1,0) \neq 0$ pues $A_i(0,0) = 0$. En particular, el conjunto de los símbolos en la posición $(1,0)$,
$\{A_i(1,0) \colon i \in \{1, \ldots, k\}\}$ debe ser un subconjunto de $\{1, \ldots, n-1\}$. Si $k \geq n$, entonces hay deben haber dos elementos repetidos en el conjunto, es decir

$$A_i(1,0) = A_j(1,0) = r,$$

para cierto $i \neq j$, y cierto $r \in \mathbb{Z}_n$. Pero entonces la superposición de A_i con A_j tendría el par (r, r) dos veces: Una vez en la posición $(0, r)$ y otra en la posición $(1, 0)$. Esto contradice la ortogonalidad de A_i y A_j. □

Luego, sabemos que para q potencias de primo, $N(q) = q-1$. Esto tiene relación con los planos afines que se definieron en auxiliar.

Recuerdo: Un plano afín de orden q es un $S_1(2, q, q^2)$ simple. De las condiciones de divisibilidad, sabemos que $r = q+1$, $m = q(q+1)$, y además se puede probar que para todo punto x, y toda linea A existe una única linea A paralela a A (Es decir, igual o disjunta) que contiene a x, y que toda linea tiene exactamente q lineas paralelas (incluyéndola). En auxiliar se vio como construir un plano afin de orden q a partir de un plano proyectivo y viceversa.

Teorema 12. *$N(q) = q-1$ si y solo si existe un plano proyectivo (o afin) de orden q.*

Demostración. Suponga que L_i, $1 \leq i \leq q$ son es un conjunto de k MOLS de orden q. Definamos $\mathcal{V} = \mathbb{Z}_q^2$ como el conjunto de las q^2 posiciones. Definamos los siguientes bloques:

$$\begin{aligned} S(i,k) &= \{(a,b) \in \mathbb{Z}^n \colon L_i(a,b) = k\} \quad \text{color } k \text{ del tablero } i \\ H(a) &= \{(a,b) \colon b \in \mathbb{Z}_n\} \quad \text{fila } a \\ V(b) &= \{(a,b) \colon a \in \mathbb{Z}_n\} \quad \text{col. } b \end{aligned}$$

Llamando $\mathcal{E} = \{H(a) \colon a \in \mathbb{Z}_n\} \cup \{V(b) \colon b \in \mathbb{Z}_n\} \cup \bigcup_{i \in \mathbb{Z}_n} \{S(i,k) \colon k \in \mathbb{Z}_n\}$, tenemos que el diseño $(\mathcal{V}, \mathcal{E})$ es q-uniforme, tiene q^2 puntos, $q(q-1) + 2q = q(q+1)$ bloques .
Veamos que $(\mathcal{V}, \mathcal{E})$ es $(2,1)$-balanceado. Consideremos un par de puntos (a,b) y (a',b') distintos de $\mathcal{V}$. Veamos que existe a lo más un bloque que contiene a ambos. Si están en la misma fila o columna, esto es claro, así que supongamos que no están en la misma fila ni columna. Si existieran 2 bloques que los contienen, digamos $S(i,k)$ y $S(j,\ell)$, entonces

$$L_i(a,b) = k = L_i(a',b'), L_j(a,b) = \ell = L_j(a',b'),$$

con lo cual la sobreposicion de L_i con L_j tiene el par (k,ℓ) en las posiciones (a,b) y (a',b'), lo que es una contradiccion.
Hemos probado que cada par de puntos están en a lo más un bloque. Como hay exactamente $q(q+1)$ bloques, cada uno de ellos teniendo q puntos (es decir $\binom{q}{2}$ pares), sabemos que hay $q(q+1)q(q-1)/2 = q^2(q^2-1)/2$ pares de puntos que definen bloques. Como esto es igual a $\binom{|\mathcal{V}|}{2}$ se concluye que cada par de puntos está en exactamente un bloque.
Con esto, $(\mathcal{V}, \mathcal{E})$ es un plano afin de orden q. Para la recíproca tomemos un plano afín $(\mathcal{V}, \mathcal{E})$ de orden q. Sean L y L' dos lineas no paralelas y llamemos $H = \{H(0), H(1), \ldots, H(q-1)\}$ (por horizontal) a las q lineas paralelas a L y $V = \{V(0), V(1), \ldots, V(q-1)\}$ (por vertical) a las q lineas paralelas a L'. Llamemos además $E_i = \{E_i(0), E_i(1), \ldots, E_i(q-1)\}$, con $1 \leq i \leq q-1$ a las otras $q-1$ clases de paralelismo del plano afín.

Con esto podemos etiquetar (coordinatizar) los elementos de $\mathcal{V}$. Es decir, podemos considerar $\mathcal{V} = \mathbb{Z}_q \times \mathbb{Z}_q$, donde (i,j) es el único punto de $\mathcal{V}$ que pertenece a $H(i) \cap V(j)$.
Para finalizar, para $1 \leq i \leq q-1$, y todo $(a,b) \in \mathcal{V}$, definimos $L_i(a,b) = c$ donde c es el único índice tal que $(a,b) \in E_i(c)$. Es fácil ver que $\{L_1, \ldots, L_{q-1}\}$ son $q-1$ MOLS de orden q. □

Volvamos al problema de los oficiales de Euler. En nuestra notación, el problema tiene solución para n si $N(n) \geq 2$.

Teorema 13. *Si n es impar, $N(n) \geq 2$.*

Demostración. Notemos que si $n \geq 3$ entonces en $\mathbb{Z}_n$, los número 1 y $-1 \equiv (n-1)$ son invertibles y distintos. Luego los tableros $A := A^{(1,n)}$ y $B := A^{(n-1,n)}$ son cuadrados latinos. Veamos que son ortogonales. Recordemos que $A(i,j) = i + j$ y que $B(i,j) = j - i$. Supongamos que en el tablero superpuesto hay un par que aparece dos veces, digamos:

$$(i+j, j-i) = (a_{ij}, b_{ij}) = (a_{k\ell}, b_{k\ell}) = (k+\ell, \ell-k),$$

de aquí se deduce que $i + j = k + \ell, j - i = \ell - k$. Sumando y restando se tiene que $2j = 2\ell$ y que $2i = 2k$. Como n es par, 2 es invertible, y esto implica que $j = \ell$ y que $i = k$. □

A continuación veremos un resultado importante de MacNeish. Para esto es útil definir una noción de producto de Kronecker de dos matrices. Si A es una matriz de orden n cuyas filas, columnas y símbolos están indexados por $\mathbb{Z}_n$ y B es una matriz de orden m indexada por $\mathbb{Z}_m$, entonces la matriz $A \otimes B$ es la matriz indexada por $\mathbb{Z}_n \times \mathbb{Z}_m$ tal que

$$A \otimes B((x,y),(z,w)) = (A(x,z), B(y,w))$$

Teorema 14 (MacNeish)**.** *(i)* $\forall n, m \geq 2, N(nm) \geq \min\{N(n), N(m)\}$

(ii) Si la factorización prima de n es $n = \prod_{i=1}^{r} p_i^{e_i}$, entonces

$$N(n) \geq \min_{1 \leq i \leq r} (p_i^{e_i} - 1).$$

Demostración. Primero veamos que (i) implica (ii). En efecto, por inducción y usando que para potencias de primos, $N(q) = q - 1$,

$$N(n) \geq \min_{1 \leq i \leq r} N(p_i^{e_i}) = \min_{1 \leq i \leq r} (p_i^{e_i} - 1).$$

Ahora probemos (i). Sean $\{A_i\}_{i=1}^k$ un conjunto de MOLS de orden n y $\{B_i\}_{i=1}^k$ un conjunto de MOLS de orden m. Entonces:

1. $A_i \otimes B_i$ es un cuadrado latino de orden nm (reindexando se puede hacer tablero). En efecto,

$$A_i \otimes B_i((x,y),(z,w)) = A_i \otimes B_i((x,y),(z',w')) \iff (A_i(x,z), B_i(y,w)) = (A_i(x,z'), B_i(y,w')) \iff (z,w) = (z',w').$$

$$A_i \otimes B_i((x,y),(z,w)) = A_i \otimes B_i((x',y'),(z,w)) \iff (A_i(x,z), B_i(y,w)) = (A_i(x',z), B_i(y',w)) \iff (x,y) = (x',y').$$

2. $A_i \otimes B_i$ es ortogonal con $A_j \otimes B_j$. En efecto,

$$\begin{aligned}
&(A_i \otimes B_i((x,y),(z,w)), A_j \otimes B_j((x,y),(z,w))) = (A_i \otimes B_i((x',y'),(z',w')), A_j \otimes B_j((x',y'),(z',w'))) \\
&\iff ((A_i(x,z), B_i(y,w)), (A_j(x,z), B_j(y,w))) = ((A_i(x',z'), B_i(y',w')), (A_j(x',z'), B_j(y',w'))) \\
&\iff (A_i \star A_j(x,z), B_i \star B_j(y,w)) = (A_i \star A_j(x',z'), B_i \star B_j(y',w')) \\
&\iff ((x,z),(y,w)) = ((x',z'),(y',w'))
\end{aligned}$$

□

Usando el teorema anterior podemos deducir lo siguiente.

Teorema 15. *Si $n \geq 4$ es múltiplo de 4, entonces $N(n) \geq 2$.*

Demostración. Escribamos $n = 2^a b$ con b impar, y $a \geq 2$. Por el teorema de MacNeish, $N(n) \geq \text{mín}\{N(2^a), N(b)\}$ Como $N(2^a) = 2^a - 1 \geq 3$, y $N(b) \geq 2$, se concluye. □

Con esto tenemos que para todo $n \geq 3$ tal que $n \not\equiv 2 \pmod 4$, $N(n) \geq 2$. El caso $n \equiv 2 \pmod 4$, con $n \geq 10$ fue resuelto afirmativamente $N(n) \geq 2$ por una multitud de autores, pero sus construcciones nos tomarían bastante tiempo. Enuciamos el siguiente teorema sin demostración.

Teorema 16. *Si* $n \in \mathbb{N} \setminus \{0, 1, 2, 6\}$, $N(n) \geq 2$. *Además* $N(2) = N(6) = 1$.