Inequalities for matrices and the $L$-intersecting problem

Richard M. Wilson
California Institute of Technology
Pasadena, CA 91125, USA

Systems of Lines
WPI, August 10, 2015
The $L$-intersecting problem

Given a set $L = \{\ell_1, \ell_2, \ldots, \ell_s\}$ of integers, a family $\mathcal{F}$ of subsets is said to be $L$-intersecting when $|A \cap B| \in L$ for all $A, B \in \mathcal{F}$, $A \neq B$. How large can such a family $\mathcal{F}$ be when $\mathcal{F}$ is a $k$-uniform family of subsets of an $n$-set?

I am especially interested in the case when $L$ and $k$ are fixed and $n$ is large or medium. It would be nice if the answer is of the form $O(n^e)$ for some $e$ depending on $L$ and $k$.

**Theorem 1 (RC-W)** If $\mathcal{F}$ is a $k$-uniform $L$-intersecting family of subsets of an $n$-set, then

$$|\mathcal{F}| \leq \binom{n}{s}.$$
Ph. Delsarte proposed a “linear programming bound” (LPB) for cliques in association schemes that can be applied to the $L$-intersecting problem. A linear program can be run given the parameters $L$, $k$, and $n$ to compute an upper bound. The LPB can be shown to be at least as good as the bound $\binom{n}{s}$, and is often dramatically better!
For example, suppose $L = \{1, 3, 6, 8, 12, 13, 16, 17\}$ and $n = 100$.

\[
\text{RC - W} \quad |F| \leq \binom{100}{8} = 186087894300
\]

LPB when $k = 39 \quad |F| \leq 1852.71$

LPB when $k = 34 \quad |F| \leq 328578.7$
But an idea of P. Frankl and W. can sometimes beat the LPB. Again, suppose $L = \{1, 3, 6, 8, 12, 13, 16, 17\}$ and $n = 100$.

\[
\begin{align*}
\text{RC} - \text{W} & \quad |F| \leq \binom{100}{8} = 186087894300 \\
\text{LPB when } k = 39 & \quad |F| \leq 1852.71 \\
\text{LPB when } k = 34 & \quad |F| \leq 328578.7 \\
\text{FW when } k \equiv 4 \pmod{5} & \quad |F| \leq \binom{100}{3} = 161700
\end{align*}
\]
For $L = \{1, 3, 6, 8, 12, 13, 16, 17\}$ and general $n$,

RC – W \quad |\mathcal{F}| \leq \binom{n}{8}

LPB when $k = 39$ \quad |\mathcal{F}| \leq \mathbf{?}

LPB when $k = 34$ \quad |\mathcal{F}| \leq \mathbf{?}

FW when $k \equiv 4 \pmod{5}$ \quad |\mathcal{F}| \leq \binom{n}{3}$
Similar theorems

**Theorem 2 (Delsarte et. al.)** If $F$ is a two-distance set on the sphere in $\mathbb{R}^d$, then

$$|F| \leq \binom{d+2}{2} - 1.$$ 

**Theorem 3 (Gerzon)** If $F$ is a set of $n$ equiangular lines through the origin in $\mathbb{R}^d$, then

$$|F| \leq \binom{d+1}{2}.$$
The RC-W and F-W inequalities can be explained in terms of the intersection matrix of a family $\mathcal{F}$ of sets. This is the matrix $M$ whose rows and columns are indexed by the members of $\mathcal{F}$ and where the entry $M(A, B)$ in row $A$ and column $B$ is $|A \cap B|$.

In thinking about these and other inequalities again, I wondered what might be said in general about the relation between rank and the number of distinct off diagonal elements of matrices. Here are a few simple observations.
Theorem 4 If $M$ is matrix of order $n$ with rank $r$ such that the number of distinct values off the diagonal is $s$ and none of these values appear on the diagonal, then

$$n \leq \binom{r + s}{s}.$$

For any matrix $M$ and any polynomial $f$, let $f(M)$ denote the matrix obtained from $M$ by applying $f$ to each entry of $M$. 
Proof. For a matrix $M$, let $M^\circ j$ denote the Hadamard product $M \circ M \circ \cdots \circ M$ with $k$ factors. If $b_1, \ldots, b_r$ is a basis for the row space of $M$, then a spanning set for the row space of $M^\circ j$ is provided by all Hadamard products

$$b_{i_1} \circ b_{i_2} \circ \cdots \circ b_{i_j}$$

of $j$ of the basis rows of $M$. So the rank of $M^\circ j$ is at most \( \binom{r+j-1}{j} \). If

$$f(x) = c_dx^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$$

is a polynomial of degree $d$, then

$$f(M) = c_dM^\circ d + c_{d-1}M^\circ(d-1) + \cdots + c_1M + c_0J$$
and hence the rank of $f(M)$ is at most

$$(r + d - 1) + (r + d - 2) + \ldots + r + 1 = (r + d).$$

(More generally, the rank of $f(M)$ is bounded above by the sum of $\binom{r+i-1}{i}$ over those $i$ for which $c_i \neq 0$.)

Anyway, if we take

$$f(x) = (x - \ell_1)(x - \ell_s) \cdots (x - \ell_s)$$

where the $\ell_i$'s are the off diagonal entries, then $F(M)$ is diagonal with nonzero diagonal entries, and so has rank $n$. $\square$
For example, when $s = 1$, we have $n \leq r + 1$, or $r \geq n - 1$.

When $s = 2$ (e.g. when $M$ is the adjacency matrix of a graph with no vertices of degree 0 or 1), $n \leq \frac{1}{2}(r + 1)(r + 2)$, which implies

$$r + 2 \geq \sqrt{2n}.$$

Any eigenvalue $\lambda \neq -1, 0, +1$ of a $(0,1)$-matrix $M$ cannot have multiplicity greater than $n + 2 - \sqrt{2n}$. 
This theorem gives approximations to Theorems 1, 2, and 3.

If \( M \) is the intersection matrix of an \( L \)-intersecting family \( \mathcal{F} \) of subsets of an \( m \)-set, where \( |L| = s \) and so sets have sizes in \( L \), then \( M = N^T \top N \) where \( N \) is the point-set incidence matrix of the family and has rank at most \( m \). Thus the size \( |\mathcal{F}| \) of \( M \) is at most \( \binom{m+s}{s} \).

But see below. E.g. When \( \mathcal{F} \) is \( k \)-uniform, the row space of \( M \) contains the vector of all 1’s, so \( |\mathcal{F}| \leq \binom{m}{s} \).

When \( F \) is a spherical 2-distance set in \( \mathbb{R}^d \), let \( N \) be the matrix whose rows are the vectors in \( F \). Then \( M = NN^\top \) has two distinct entries, so its size \( |F| \) cannot exceed \( \binom{d+2}{2} \).
When $F$ is a equiangular set of lines in $\mathbb{R}^d$, let $N$ be the matrix whose rows consist of one unit vector from each line. Then $M = NN^\top$ has two off-diagonal entries, $c$ and $-c$ for some $c$. so its size $|F|$ cannot exceed $\binom{d+2}{2}$.

[The polynomial $(x - c)(x + c)$ has no $x$-term, so this last bound can be instantly improved to $\binom{d+2}{2} - d$.]
Generalizations

Theorem 5  If \( M \) is matrix of order \( n \) with rank \( r \) such that the number of distinct values above the diagonal is \( s \) and none of these values appear on the diagonal, then

\[
n \leq \binom{r + s}{s}.
\]

Theorem 6  Let \( M \) be a matrix of order \( n \) with rank \( r \) such that the number of distinct values above the diagonal is \( s \) and none of these values appear on the diagonal. If the vector of all 1's belongs to the row space of \( M \), then

\[
n \leq \binom{r}{s}.
\]
**Theorem 7** If $M$ is a $(0, 1)$-matrix of order $n$ with rank $r$ such that the number of distinct values above the diagonal is $s$ and none of these values appear on the diagonal, then

$$n \leq \binom{r}{s} + \binom{r}{s-1} + \cdots + r + 1.$$ 

**Theorem 8** Let $M$ is a $(0, 1)$-matrix of order $n$ with rank $r$ such that the number of distinct values above the diagonal is $s$ and none of these values appear on the diagonal. Then

$$n \leq \binom{r}{s}.$$ 

The same conclusion holds if the row space of $M$ is spanned by its $(0, 1)$-vectors.

We can deduce the full Theorems 1, 2, and 3 by refining the arguments above. Unfortunately, this slide is too small to contain
The $L$-intersection Problem Again

**Theorem 9** (FW) Let $L = \{\ell_1, \ell_2, \ldots, \ell_s\}$. Suppose there exists a rational polynomial $f(x)$ of degree $d$ and a prime $p$ so that

$$f(\ell_i) \equiv 0 \pmod{p} \quad \text{for } i = 1, 2, \ldots, s, \quad \text{but} \quad f(k) \not\equiv 0 \pmod{p}. \quad (1)$$

Then for an $L$-intersecting $k$-uniform family $\mathcal{F}$

$$|\mathcal{F}| \leq \binom{n}{d}.$$

Note that $f$ is required to take integer values on $k$ and the $\ell_i$’s, but need not be integer-valued in general.

Idea of proof: Let $M$ be the intersection matrix. Then $f(M)$ is nonsingular modulo $p$ and hence nonsingular.
A corollary with $f(x) = (x - \ell_1)(x - \ell_2)\ldots(x - \ell_r)$ is

**Corollary 10** *If $k$ is not congruent to any of $\ell_1, \ell_2, \ldots, \ell_r$ modulo $p$ but $|A \cap B|$ is congruent to one of $\ell_1, \ell_2, \ldots, \ell_r$ modulo $p$ for all distinct $A, B \in \mathcal{F}$, then*

$$|\mathcal{F}| \leq \binom{n}{r}.$$  

Example: If $k$ is even and the elements of $L$ are odd, then $|\mathcal{F}| \leq n$. Use $f(x) = x - 1$ and $p = 2$. 
Suppose \( L = \{1, 3, 6, 8, 12, 13, 16, 17\} \) and \( n = 100 \).

\[
\begin{align*}
\text{RC} - \text{W} & \quad |\mathcal{F}| \leq \binom{100}{8} = 186087894300 \\
\text{LPB when } k = 39 & \quad |\mathcal{F}| \leq 1852.71 \\
\text{LPB when } k = 34 & \quad |\mathcal{F}| \leq 328578.7 \\
\text{FW when } k \equiv 4 \pmod{5} & \quad |\mathcal{F}| \leq \binom{100}{3} = 161700
\end{align*}
\]
Theorem 11 (Keevash-Mubayi-W), 2006 Let $\mathcal{F}$ be a 1-avoiding $k$-uniform family of subsets of an $n$-set, $k \geq 3$. Then $\mathcal{F} \leq \binom{n}{k-2}$.

Proof. Take $f(x) = \binom{x-2}{k-2}$. Then $f(k) = 1$, 

$$f(k-1) = f(k-2) = \cdots = f(3) = f(2) = 0, \quad f(0) = \pm (k-1).$$

Choose $p$ as any prime divisor of $k-1$. \qed
Theorem 12 If $k - t = p^e$ for some prime $p$ and positive integer $e$, and if $\mathcal{F}$ is $k$-uniform and $t$-avoiding with $k \geq 2t$, then

$$|\mathcal{F}| \leq \binom{n}{k - t}.$$ 

Remark: This bound is weaker than that of the Frankl-Füredi Theorem, but it holds for all $n$, not just sufficiently large $n$.

Proof. Let $f(x) = \binom{x - t}{k - t}$. Then $f(k) = 1,$

$$f(k - 1) = f(k - 2) = \cdots = f(t) = 0,$$

and

$$f(t - j) = \binom{-j}{k - t} = (-1)^{k-t}\binom{k-t+j-1}{k-t} \equiv 0 \pmod{p}$$

for $j = 2, 3, \ldots, k - t - 1$. \qed
As an example, when \( s = 2 \) and \( |A \cap B| \in \{\alpha, \beta\} \), Theorem 1 says \( |\mathcal{F}| \leq \binom{n}{2} \). But if there exists a prime divisor \( p \) of \( \beta - \alpha \) that does not divide \( k - \alpha \), we may use the polynomial \( f(x) = x - \alpha \) in Theorem 9 to deduce \( |\mathcal{F}| \leq n \). More generally, if the \( p \)-contribution to \( k - \alpha \) is \( p^e \) but the \( p \)-contribution to \( \beta - \alpha \) is higher, we may consider the rational polynomial \( f(x) = (x - \alpha)/p^e \). In summary,

\[
|\mathcal{F}| \leq \binom{n}{2} \quad \text{and in fact} \quad |\mathcal{F}| \leq n \quad \text{unless} \quad (\beta - \alpha) | (k - \alpha).
\]

We remark that if \( \beta - \alpha \) does divide \( k - \alpha \), there exists a \( \{\alpha, \beta\} \)-intersecting family of \( cn^2 \) \( k \)-subsets.
When $d$ is chosen to be the least integer for which (1) holds for some rational polynomial $f(x)$ and prime $p$, we may call the upper bound $\binom{n}{d}$ the “modular bound” (MB) for $|\mathcal{F}|$.

The MB uses only the values of $k$ and the $\ell_i$’s, and gives a bound valid for all $n$. There are numerous instances when the MB is better than the LPB, and many where the LPB is better.

Example: Let $L = \{4, 7\}$ and $k \equiv 1 \pmod{3}$. Start with the blocks of an $S(2,(k - 4))/3,n)$. Replace each point by three points. The inflated blocks meet in 0 or 3 points. Add four new points to each inflated block. We get an $L$-intersecting $k$-uniform family of $cn^2$ subsets of a $(3n + 4)$-set.
Do good polynomial-prime pairs exist?

The following is part of joint work with Tian Nie.

**Theorem 13** Let integers $k$ and $\ell_1, \ell_2, \ldots, \ell_s$ be given. There exists a rational polynomial $f(x)$ of degree $d$ and a prime $p$ so that (1) holds if and only if the vector $(1, k, k^2, \ldots, k^d)$ is NOT an integer linear combination of the rows

$$(1, \ell_i, \ell_i^2, \ldots, \ell_i^d), \quad i = 1, 2, \ldots, s.$$ 

This follows from well-known necessary and sufficient conditions for the existence of solutions of systems of equations in integers.
For a $m$ by $n$ integer matrix $A$ with $m \leq n$, we use the term
content of $A$ for the product of the $m$ invariant factors of $A$, and we denote this by $\kappa(A)$. This is the same as $\text{GCD}$ of the
$m$ by $m$ submatrices of $A$. It is the order of the abelian group
$\mathbb{Z}^m/\text{col}_{\mathbb{Z}}(A)$. It may be computed using algorithms for Smith
normal form.

**Theorem 14** Let integers $k$ and $\ell_1, \ell_2, \ldots, \ell_s$ be given. For $d \leq s$, the vector $(1, k, k^2, \ldots, k^d)$ is a integer linear combination of the rows

$$(1, \ell_i, \ell_i^2, \ldots, \ell_i^d), \quad i = 1, 2, \ldots, s$$

if and only if the content $G_0$ of $M = (\ell_i^j)$ is the same as the content $G_1$ of the matrix $M^*$ obtained by appending $(1, k, k^2, \ldots, k^d)$ to $M$. 
This is because the order of $\text{row}_Z(M')/\text{row}_Z(M)$ is $\kappa(M)/\kappa(M')$.

**Theorem 15** There exists a rational polynomial $f(x)$ of degree $\leq s - 1$ and a prime $p$ so that

\[ f(\ell_i) \equiv 0 \pmod{p} \quad \text{for } i = 1, 2, \ldots, s, \quad \text{but} \quad f(k) \not\equiv 0 \pmod{p}. \quad (*) \]

if and only if for some $j$, $1 \leq j \leq s$,

\[ \prod_{i: i \neq j} (\ell_j - \ell_i) \quad \text{does NOT divide} \quad \prod_{i: i \neq j} (k - \ell_i). \]
Example: $s = 2$, $L = \{\alpha, \beta\}$. An improved bound $|\mathcal{F}| \leq n$ will hold unless both

$$\alpha - \beta \mid k - \beta \quad \text{and} \quad \beta - \alpha \mid k - \alpha$$

hold. (They are equivalent.)

Example: $s = 3$, $L = \{\alpha, \beta, \gamma\}$. An improved bound $|\mathcal{F}| \leq \binom{n}{2}$ will hold unless all of

$$(\alpha - \beta)(\alpha - \gamma) \mid (k - \beta)(k - \gamma)$$

$$(\beta - \alpha)(\beta - \gamma) \mid (k - \alpha)(k - \gamma)$$

$$(\gamma - \alpha)(\gamma - \beta) \mid (k - \alpha)(k - \gamma)$$

hold.
Remark: If \( L \) consists of a set of \( s \) consecutive integers, then there are no polynomials of degree \( < s \) that can be used in (1). This follows from Theorem 15 and also because we can construct \( k \)-uniform \( L \)-intersecting families of \( cn^s \) subsets of \( n \)-sets.

For example, if \( L = \{2, 3, 4, 5\} \) and \( k = 9 \), and \( L \)-intersecting 9-uniform family \( \mathcal{F} \) can be obtained by adding two new points to each block of a Steiner system \( S(4, 7, n - 2) \), and for this family \( |\mathcal{F}| = cn^4 \).
The case $k = 10$, $s = 3$. Of the 120 relevant 3-subsets $L$, whether the bound $O(n^2)$ holds is settled in all but 15 instances. For 11 choices of $L$, there exist $c n^3$ 10-subsets. For 94 choices of $L$, $|\mathcal{F}| \leq \binom{n}{2}$. The 15 unsettled cases are

$$\{0, 1, 3\}, \{0, 1, 6\}, \{0, 4, 6\}, \{1, 2, 4\}, \{1, 2, 5\},$$
$$\{1, 3, 4\}, \{1, 5, 6\}, \{2, 4, 5\}, \{2, 4, 8\}, \{2, 5, 7\},$$
$$\{3, 4, 6\}, \{3, 6, 7\}, \{4, 5, 7\}, \{5, 7, 8\}, \{6, 7, 9\}.$$

When $L = \{0, 1, 3\}$, we have $|\mathcal{F}| \leq \binom{n}{2}$ when $k \equiv 2 \pmod{3}$. When $k = 7$ and $k = 9$, the inequality $|\mathcal{F}| \leq \binom{n}{2}$ fails infinitely often (planes of projective spaces over $\mathbb{F}_2$ and affine spaces over $\mathbb{F}_3$). But $k = 10$ is open.