Some applications of linear algebra over finite fields

Let A be a non-singular $k \times k$ matrix over $\mathbb{F}_q$.

[Jaeger 1981 conjecture]
If $q \geq 4$ then there exists an $x \in \mathbb{F}_q^k$ such that x and Ax have no zero coordinate.

Let A be a non-singular $k \times k$ matrix over $\mathbb{F}_q$.

[Jaeger 1981 conjecture]
If $q \geq 4$ then there exists an $x \in \mathbb{F}_q^k$ such that x and Ax have no zero coordinate.

Not true $q = 2$, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $q = 3$, $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Let A be a non-singular $k \times k$ matrix over $\mathbb{F}_q$.

[Jaeger 1981 conjecture]
If $q \geq 4$ then there exists an $x \in \mathbb{F}_q^k$ such that x and Ax have no zero coordinate.

Not true $q = 2$, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $q = 3$, $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

[Alon and Tarsi 1989]
True for q not prime.

Let $B = \{e_1, \ldots, e_k\}$ be a basis of $\mathbb{F}_q^k$ and let f be the endomorphism which has matrix A with respect to B.

Define linear maps α_i from $\mathbb{F}_q^k$ to $\mathbb{F}_q$ by

$$f(x) = \sum_{i=1}^{k} \alpha_i(x) e_i.$$

Let $B = \{e_1, \dots, e_k\}$ be a basis of $\mathbb{F}_q^k$ and let f be the endomorphism which has matrix A with respect to B.

Define linear maps α_i from $\mathbb{F}_q^k$ to $\mathbb{F}_q$ by

$$f(x) = \sum_{i=1}^{k} \alpha_i(x) e_i.$$

Define a function $p(x)$ from $\mathbb{F}_q^k$ to $\mathbb{F}_q$ by

$$p(x) = \prod_{i=1}^{k} \alpha_i(x).$$

Assume that $p(x) = 0$, whenever $\prod_{i=1}^{k} x_i \neq 0$, where $x = (x_1, \dots, x_k)$ are the coordinates of x with respect to B.

By Alon's Nullstellensatz, $p = \sum (X_i^{q-1} - 1) h_i(X)$, for some polynomials h_i of degree at most $k - q + 1$.

With respect to the dual basis $\{\alpha_1, \ldots, \alpha_k\}$, the monomials $X_i = \sum c_{ij}\alpha_j$, for some c_{ij}.

Thus

$$p = \prod_{i=1}^{k} \alpha_i = \sum ((\sum c_{ij}\alpha_j)^{q-1} - 1) h_i,$$

which gives a contradiction for q non-prime, since $(q-1)! = 0$.

Let $q = p^h$, where p is a prime.

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ a_1 & a_2 & \dots & a_q & \vdots \\ \vdots & & & \vdots & 0 \\ a_1^{k-1} & a_2^{k-1} & \dots & a_q^{k-1} & 1 \end{pmatrix}$$

is a $k \times (q+1)$ matrix,

every k columns are linearly independent over $\mathbb{F}_q$.

Let $q = p^h$, where p is a prime.

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ a_1 & a_2 & \dots & a_q & \vdots \\ \vdots & & & \vdots & 0 \\ a_1^{k-1} & a_2^{k-1} & \dots & a_q^{k-1} & 1 \end{pmatrix}$$

is a $k \times (q+1)$ matrix,

every k columns are linearly independent over $\mathbb{F}_q$.

The $k \times k$ submatrices are Vandermonde and have determinants

$$\prod (a_i - a_j) \neq 0.$$

Let $q = 2^h$.

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 0 & 0 \\ a_1 & a_2 & \dots & a_q & 0 & 1 \\ a_1^2 & a_2^2 & \dots & a_q^2 & 1 & 0 \end{pmatrix}$$ is a $3 \times (q+2)$ matrix.

every 3 columns of which are linearly independent over $\mathbb{F}_q$.

Let S be a set of vectors of $\mathbb{F}_q^k$ in which every subset of S of size k is a basis.

Let S be a set of vectors of $\mathbb{F}_q^k$ in which every subset of S of size k is a basis.

How large can S be ? (at least $q+1$)

Let S be a set of vectors of $\mathbb{F}_q^k$ in which every subset of S of size k is a basis.

How large can S be ? (at least $q+1$)

[Bush 1952]
$S = \{e_1, \dots, e_k, e_1 + \dots + e_k\}$ is a set in which every subset of size k is a basis and if $k \geq q+1$ then this is best possible.

Let S be a set of vectors of $\mathbb{F}_q^k$ in which every subset of S of size k is a basis.

How large can S be ? (at least $q+1$)

[Bush 1952]
$S = \{e_1, \dots, e_k, e_1 + \dots + e_k\}$ is a set in which every subset of size k is a basis and if $k \geq q+1$ then this is best possible.

[MDS conjecture (Segre 1955)]
If $k \leq q$ then S has size at most $q+1$

Let S be a set of vectors of $\mathbb{F}_q^k$ in which every subset of S of size k is a basis.

How large can S be ? (at least $q+1$)

[Bush 1952]
$S=\{e_1,\dots,e_k,e_1+\dots+e_k\}$ is a set in which every subset of size k is a basis and if $k \geq q+1$ then this is best possible.

[MDS conjecture (Segre 1955)]
If $k \leq q$ then S has size at most $q+1$

unless $q=2^h$ and $k=3$ or $k=q-1$, in which case $|S| \leq q+2$.

Suppose $e_1, \ldots, e_{k-2}$ are in S, so in each of the $q+1$ hyperplanes, $X_{k-1} = aX_k$ and $X_k = 0$, there is at most one other vector of S.

(If not then there is a hyperplane containing a set of k vectors of S which do not form a basis)

Suppose $e_1, \ldots, e_{k-2}$ are in S, so in each of the $q+1$ hyperplanes, $X_{k-1} = aX_k$ and $X_k = 0$, there is at most one other vector of S.

(If not then there is a hyperplane containing a set of k vectors of S which do not form a basis)

So $|S| \leq k-2+q+1 = q+k-1$.

For every $e_1, \dots, e_{k-2}$ in S, there are

$$t := q + k - 1 - |S|$$

hyperplanes containing no other vectors of S.

For every $e_1, \dots, e_{k-2}$ in S, there are

$$t := q + k - 1 - |S|$$

hyperplanes containing no other vectors of S.

[Segre 1967]

In the quotient space $\mathbb{F}_q^k / \langle e_1, \dots, e_{k-3} \rangle$ the vectors dual to these hyperplanes lie on an algebraic curve of small degree.

For every $Y = \{e_1, \ldots, e_{k-2}\}$ subset of S, define a function

$$T_Y(x) = \prod f(x),$$

where the product is over the linear maps f that define the t hyperplanes containing the vectors of Y and no others from S.

For every $Y = \{e_1, \ldots, e_{k-2}\}$ subset of S, define a function

$$T_Y(x) = \prod f(x),$$

where the product is over the linear maps f that define the t hyperplanes containing the vectors of Y and no others from S.

[Segre 1967] $k = 3$. For all $x, y, z \in S$,

$$T_{\{x\}}(y)\,T_{\{y\}}(z)\,T_{\{z\}}(x) = (-1)^{t+1}\,T_{\{x\}}(z)\,T_{\{y\}}(x)\,T_{\{z\}}(y)$$

For every $Y = \{e_1, \dots, e_{k-2}\}$ subset of S, define a function

$$T_Y(x) = \prod f(x),$$

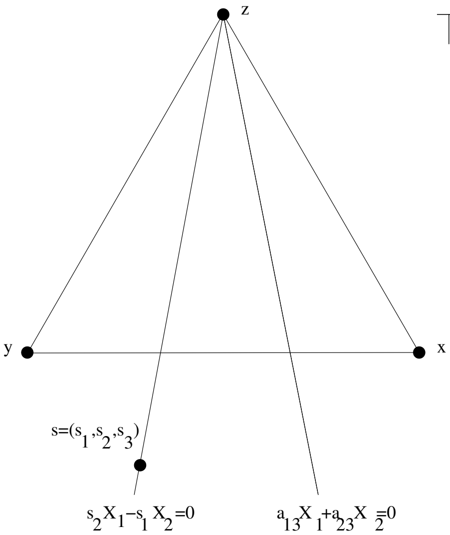
where the product is over the linear maps f that define the t hyperplanes containing the vectors of Y and no others from S.

[Segre 1967] $k = 3$. For all $x, y, z \in S$,

$$T_{\{x\}}(y)T_{\{y\}}(z)T_{\{z\}}(x) = (-1)^{t+1}T_{\{x\}}(z)T_{\{y\}}(x)T_{\{z\}}(y)$$

For any subset B of S of size $k-3$,

$$T_{B\cup x}(y)T_{B\cup y}(z)T_{B\cup z}(x) = (-1)^{t+1}T_{B\cup x}(z)T_{B\cup y}(x)T_{B\cup z}(y)$$



$$\prod \frac{s_2}{s_1} \prod \frac{a_{13}}{a_{23}} (-1)^t = -1$$

$$T_z(X) = \prod (a_{13}X_1 + a_{23}X_2)$$

$$T_z(x) = \prod a_{13}$$

$$T_z(x)T_x(y)T_y(z) = (-1)^{t+1} T_y(x)T_z(y)T_x(z)$$

With respect to the basis {x,y,z}.

For any subset B of S of size $k-3$,

$$T_{B\cup x}(y)\,T_{B\cup y}(z)\,T_{B\cup z}(x) = (-1)^{t+1}\,T_{B\cup x}(z)\,T_{B\cup y}(x)\,T_{B\cup z}(y)$$

For any subset B of S of size $k-3$,

$$T_{B\cup x}(y)T_{B\cup y}(z)T_{B\cup z}(x) = (-1)^{t+1}T_{B\cup x}(z)T_{B\cup y}(x)T_{B\cup z}(y)$$

By interpolation, for disjoint ordered sequences E of size $t+2$ and $Y=(y_1,\ldots,y_{k-2})$, subsets of S,

$$\sum_{e\in E} T_Y(e) \prod_{z\in E\setminus e} \det(z,e,y_1,\ldots,y_{k-2})^{-1} = 0.$$

Fix a $y \in Y$ and combine the $k-1$ equations given by $Y' = (Y\setminus y)\cup e$ and $E' = (E\setminus e)\cup y$, for some $e \in E$.

Combining these equations gives for $r \leq \min(k-1, t+2)$,

$$0 = \sum_{e_1,\dots,e_r \in E} \left(\prod_{i=1}^{r} \frac{T_{\theta_i}(e_i)}{T_{\theta_i}(y_{i-1})} \right) \prod_z \det(e_r, z, \theta_r)^{-1}$$

where $\theta_i = \{e_1, \dots, e_{i-1}, y_i, \dots, y_{k-2}\}$ and the product runs over the $t+1$ vectors of E and Y not in $\theta_r \cup \{e_r\}$.

.

Combining these equations gives for $r \leq \min(k-1, t+2)$,

$$0 = r! \sum_{\{e_1,\ldots,e_r\}\subseteq E} \left(\prod_{i=1}^{r} \frac{T_{\theta_i}(e_i)}{T_{\theta_i}(y_{i-1})} \right) \prod \det(e_r, z, \theta_r)^{-1}$$

where $\theta_i = \{e_1, \ldots, e_{i-1}, y_i, \ldots, y_{k-2}\}$ and $|E| = t+2$.

Combining these equations gives for $r \leq \min(k-1, t+2)$,

$$0 = r! \sum_{\{e_1,\dots,e_r\} \subseteq E} \left(\prod_{i=1}^{r} \frac{T_{\theta_i}(e_i)}{T_{\theta_i}(y_{i-1})} \right) \prod \det(e_r, z, \theta_r)^{-1}$$

where $\theta_i = \{e_1, \dots, e_{i-1}, y_i, \dots, y_{k-2}\}$ and $|E| = t+2$.

If $|S| = q+2$ then $t = k-3$, this gives a sum of just one term which is zero. Thus, $k \leq p$ gives a contradiction.

Combining these equations gives for $r \leq \min(k-1, t+2)$,

$$0 = r! \sum_{\{e_1,\ldots,e_r\} \subseteq E} \left(\prod_{i=1}^{r} \frac{T_{\theta_i}(e_i)}{T_{\theta_i}(y_{i-1})} \right) \prod \det(e_r, z, \theta_r)^{-1}$$

where $\theta_i = \{e_1, \ldots, e_{i-1}, y_i, \ldots, y_{k-2}\}$ and $|E| = t+2$.

If $|S| = q+2$ then $t = k-3$, this gives a sum of just one term which is zero. Thus, $k \leq p$ gives a contradiction.

If $|S| = q+1$ then $t = k-2$, and if $k \leq p$, we get a set of $k-2$ linearly independent equations in k unknowns, whose solution is (equivalent to)

$$S = \{(1, a, \ldots, a^{k-1}) \mid a \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\}.$$

[Conjecture] If $k \leq q$ then S has size at most $q+1$ unless $q = 2^h$ and $k=3$ or $k=q-1$, in which case $|S| \leq q+2$.

$k < \sqrt{q}/4$. q odd $k < \sqrt{q}$. q even [Segre 1967].

[Conjecture] If $k \leq q$ then S has size at most $q+1$ unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $|S| \leq q+2$.

$k < \sqrt{q}/4$. q odd $k < \sqrt{q}$. q even [Segre 1967].

$k < q/45$. $q = p$ prime. [Voloch 1990]

[Conjecture] If $k \leq q$ then S has size at most $q+1$ unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $|S| \leq q+2$.

$k < \sqrt{q}/4$. q odd $k < \sqrt{q}$. q even [Segre 1967].

$k < q/45$. $q = p$ prime. [Voloch 1990]

$k < \sqrt{pq}$. $q = p^{2h+1}$ [Voloch 1991].

[Conjecture] If $k \leq q$ then S has size at most $q+1$ unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $|S| \leq q+2$.

$k < \sqrt{q}/4$. q odd $k < \sqrt{q}$. q even [Segre 1967].

$k < q/45$. $q = p$ prime. [Voloch 1990]

$k < \sqrt{pq}$. $q = p^{2h+1}$ [Voloch 1991].

$k < \sqrt{q}/2$. $q = p^{2h}$, $p > 5$ [Hirschfeld and Korchmaros 1996].

[Conjecture] If $k \leq q$ then S has size at most $q+1$ unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $|S| \leq q+2$.

$k < \sqrt{q}/4$. q odd $k < \sqrt{q}$. q even [Segre 1967].

$k < q/45$. $q = p$ prime. [Voloch 1990]

$k < \sqrt{pq}$. $q = p^{2h+1}$ [Voloch 1991].

$k < \sqrt{q}/2$. $q = p^{2h}$, $p > 5$ [Hirschfeld and Korchmaros 1996].

$k < q$. $q = p$ prime [Ball 2010]

[Conjecture] If $k \leq q$ then S has size at most $q+1$ unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $|S| \leq q+2$.

$k < \sqrt{q}/4$. q odd $k < \sqrt{q}$. q even [Segre 1967].

$k < q/45$. $q = p$ prime. [Voloch 1990]

$k < \sqrt{pq}$. $q = p^{2h+1}$ [Voloch 1991].

$k < \sqrt{q}/2$. $q = p^{2h}$, $p > 5$ [Hirschfeld and Korchmaros 1996].

$k < q$. $q = p$ prime [Ball 2010]

$k < 2\sqrt{q}$. $q = p^2$ [Ball and De Beule 2011]

The row space of the matrix whose columns are the vectors of S is a maximum distance separable code of length $|S|$ and dimension k .

Thus, we have that the maximum length of a maximum distance separable code over $\mathbb{F}_p$ is $p+1$ and the longest ones are Reed-Solomon codes.

The row space of the matrix whose columns are the vectors of S is a maximum distance separable code of length $|S|$ and dimension k .

Thus, we have that the maximum length of a maximum distance separable code over $\mathbb{F}_p$ is $p+1$ and the longest ones are Reed-Solomon codes.

The uniform matroid of rank r and base set E, where $|E| \geq r+2$, is representable over $\mathbb{F}_p$ if and only if $|E| \leq p+1$.

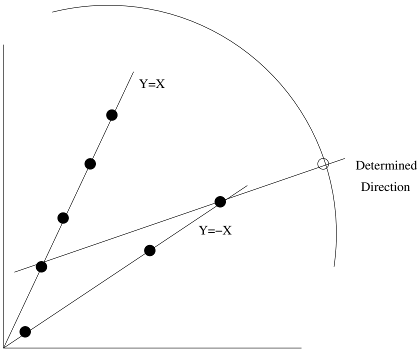
How few directions can a function over a finite field f determine ?
How small can the set $D(f)$ be ?

$$D(f) = \{\frac{f(y) - f(x)}{y - x} \mid x, y \in \mathbb{F}_q,\ x \neq y\}$$

ex. if f is linear then $|D(f)| = 1$.

ex. if f is linear over $\mathbb{F}_s \leq \mathbb{F}_q$ then
$q/s + 1 \leq |D(f)| \leq (q-1)/(s-1)$.

ex. if $f(x) = x^{(q+1)/2}$ and q is odd then $|D(f)| = (q+3)/2$.



Let p be a prime.

[Rédei 1970]
A non-linear function from $\mathbb{F}_p$ to $\mathbb{F}_p$ determines at least $(p+3)/2$ directions.

Let p be a prime.

[Rédei 1970]
A non-linear function from $\mathbb{F}_p$ to $\mathbb{F}_p$ determines at least $(p+3)/2$ directions.

[Lóvasz and Schrijver 1981]
If $|D(f)| = (p+3)/2$ then f is affinely equivalent to $x^{(p+1)/2}$.

Let p be a prime.

[Rédei 1970]
A non-linear function from $\mathbb{F}_p$ to $\mathbb{F}_p$ determines at least $(p+3)/2$ directions.

[Lóvasz and Schrijver 1981]
If $|D(f)| = (p+3)/2$ then f is affinely equivalent to $x^{(p+1)/2}$.

[Gács 2003]
If $|D(f)| > (p+3)/2$ then $|D(f)| > 2(p-1)/3$.

If $-c \notin D(f)$ then $x \mapsto f(x) + cx$ is a permutation.

Let $I(f)$ be maximum such $\sum_{x \in \mathbb{F}_p} (f(x) + xY)^k \equiv 0$ for all $k = 1, \ldots, I(f) - 1$.

Then $I(f) \geq p - |D(f)| + 1$.

[Gács]

Consider $x^i f(x)^j$ as elements of $\mathbb{F}_p(x)/(x^p - x)$.

Note that the above implies that $x^i f(x)^j$ has degree $\leq p - 2$ for all $1 \leq i + 1 \leq I(f) - 1$.

Consider linear maps

$$\phi(A_1,\dots,A_s) \mapsto \sum_{i=0}^{s} A_i(x)f(x)^i,$$

where the degree of $A_i(x)$ satisfies $\deg A_i \leq s-i$.

If $g, h \in \mathrm{Im}(\phi)$ then $\deg(gh) \neq p-1$.

If $s < I(f)/2$ then only half the degrees can occur amongst the polynomials in $\mathrm{Im}(\phi)$.

[Ball and Gács 2008] If $I(f) > (p-1)/t + t - 1$ for some $t \in \mathbb{N}$ then every line meets the graph of f in at most $t-1$ points or at least $(p-1)/t + 1$ points.

This implies that if $|D(f)| < p - 2\sqrt{p-1} + 15/4$ then the graph of f has additional properties.

[Conjecture] If $I(f) > (p-1)/t + t - 1$ for some $t \in \mathbb{N}$ then the graph of f is contained in an algebraic curve of degree $t-1$.

[Rédei 1970] True for $t = 2$.

[Gács 2003] True for $t = 3$.

Let q be a prime power.

[Ball, Blokhuis, Brouwer, Storme, Szőnyi 1999], [Ball 2003]

If $|D(f)| \leq (q+1)/2$ and s is maximal with the property that every line meets the graph of f is a multiple of s points then

$\mathbb{F}_s \leq \mathbb{F}_q$,

$q/s + 1 \leq |D(f)| \leq (q-1)/(s-1)$,

and for $s > 2$ the function f is linear over $\mathbb{F}_s$.