The Maximum Distance Separable Codes Conjecture

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

A k-dimensional linear code C over $\mathbb{F}_q$ with minimum distance d and length n is a k-dimensional subspace of $\mathbb{F}_q^n$ in which every non-zero vector has at least d non-zero coordinates.

[Singleton] (1964) $k \leq n - (d - 1)$.

If $k = n - d + 1$ then C is called maximum distance separable (MDS).

The Reed-Solomon code with generator matrix

$$G=\begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ a_1 & a_2 & \dots & a_q & \vdots \\ \vdots & & & \vdots & 0 \\ a_1^{k-1} & a_2^{k-1} & \dots & a_q^{k-1} & 1 \end{pmatrix}$$ is an MDS code.

For all $x \in \mathbb{F}_q^k$ the vector xG has at most $k-1$ zeros.
So $d \geq n-(k-1)$ and hence $d = n-k+1$.

So there exist linear MDS codes over $\mathbb{F}_q$ of length $n = q+1$.

So there exist linear MDS codes over $\mathbb{F}_q$ of length $n = q + 1$.

The $k \times k$ identity matrix with the all-1 column vector appended generates an MDS code of length $k + 1$.

[Bush] (1952)
If $k \geq q + 1$ then this is best possible,. Hence $n \leq k + 1$.

[Segre] (1955) The MDS conjecture
If $k \leq q$ then $n \leq q + 1$,

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

Let $q = 2^h$.

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 & 0 \\ a_1 & a_2 & \dots & a_q & 0 & 1 \\ a_1^2 & a_2^2 & \dots & a_q^2 & 1 & 0 \end{pmatrix}$$

generates a linear MDS code over $\mathbb{F}_q$ of length $q + 2$.

[Exercise] G is the generator matrix of a k-dimensional MDS code iff every set of k columns of G is a basis of $\mathbb{F}_q^k$.

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

To prove the MDS conjecture we have to show that S has size at most $q+1$ for all $k \leq q$,

unless $q = 2^h$ and $k = 3$ or $k = q - 1$, in which case we want to show that S has size at most $q + 2$.

Suppose $e_1, \dots, e_{k-2}$ 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 $Y \subset S$ of size $k-2$, there are

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

hyperplanes of $\mathbb{F}_q^k$ containing Y and no other vectors of S.

For every $Y \subset S$ of size $k-2$, there are

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

hyperplanes of $\mathbb{F}_q^k$ containing Y and no other vectors of S.

[Segre] (1967) [Blokhuis et al.] (1990)

The $\binom{|S|}{k-2} t$ vectors dual to these hyperplanes lie on an algebraic hypersurface of small degree.

For every $Y \subset S$ of size $k-2$, define a function

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

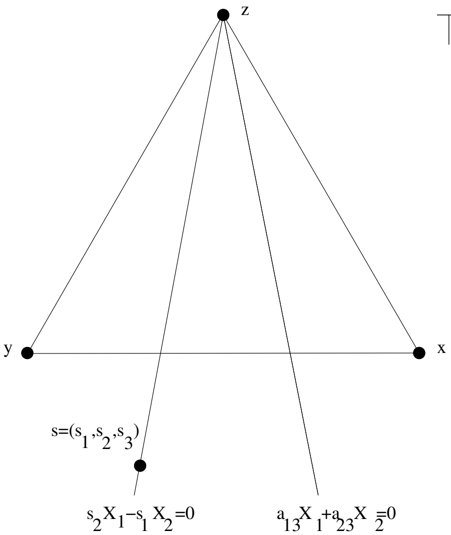
where the product is over the t linear maps f whose kernels are the t hyperplanes containing the vectors of Y and no others from S.

[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 $B \subset S$ 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 every $D \subset S$ of size $k - 1 - n$,

Segre's Lemma implies that changing the order of two elements of $A = \{a_1, \ldots, a_n\}$ (or $B = \{b_0, \ldots, b_{n-1}\}$)
changes the sign of the product

$$P_D(A, B) = \prod_{i=1}^{n} \frac{T_{D \cup \{a_1, \ldots, a_{i-1}, b_i, \ldots, b_{n-1}\}}(a_i)}{T_{D \cup \{a_1, \ldots, a_{i-1}, b_i, \ldots, b_{n-1}\}}(b_{i-1})}$$

by $(-1)^{t+1}$.

By interpolation, for disjoint ordered sequences $E = (e_1, \ldots, e_{t+2})$ and $Y = (y_1, \ldots, y_{k-2})$ of S,

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

Let p be the characteristic of the field.

By induction for $r = 1, \dots, \min(p-1, t+2)$,

$$0 = \sum_{\substack{\Delta\subseteq E\\ |\Delta|=r}} P_D(\Delta, L) \prod_{z\in(E\setminus\Delta)\cup(L\setminus\ell_0)} \det(z, \Delta, D)^{-1},$$

where $|L| = r$, $|D| = k-1-r$ and ℓ_0 is the first element of L.

If $|S| = q+2$ then $t = k-3$. Thus, if $k \leq p$ put $r = t+2$ and this sum has just one term, a contradiction.

So when $q = p$ the MDS conjecture is true.

Moreover, putting $|S| = q+1$ one can prove that for $k \leq p$ the longest MDS codes are Reed Solomon.

[MDS Conjecture] If $k \leq q$ then a linear MDS code has length $n \leq q+1$ unless $q = 2^h$ and $k = 3$ or $k = q-1$, in which case $n \leq q+2$.

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

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

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

$k < q$. $q = p$ [Ball] (2010)

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