On Maximum Distance Separable Codes

Simeon Ball
Universitat Politècnica Catalunya,
Barcelona
A block code $C$ of length $n$ and minimum distance $d$ over an alphabet of size $r$ satisfies

$$|C| \leq r^{n-d+1}.$$ 

If $|C| = r^{n-d+1}$ then $C$ is maximum distance separable (MDS).

A $k$-dimensional linear code $C$ over $\mathbb{F}_q$ with minimum distance $d$ and length $n$

$$k \leq n - d + 1.$$ 

If $k = n - d + 1$ then $C$ is a linear MDS code.
Example: The $k$-dimensional Reed-Solomon code is the evaluation of all polynomials of degree at most $k - 1$ in $\mathbb{F}_q \cup \{\infty\}$.

It has a generator matrix

$$
\begin{pmatrix}
1 & 1 & \ldots & 1 & 0 \\
1 & a_1 & a_2 & \ldots & a_q \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & a_{k-1}^{k-1} & a_{k-1}^{k-2} & \ldots & a_{k-1}^1 \\
\end{pmatrix}
$$

So if $k \leq q$ then 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 $k \geq q$ then this is best possible. Hence $n \leq k + 1$ and $d \leq 2$.

[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 $q = 2^h$ and let $e$ be co-prime to $h$.

The matrix

\[
G = \begin{pmatrix}
1 & 1 & \ldots & 1 & 0 & 0 \\
\alpha_1 & \alpha_2 & \ldots & \alpha_q & 0 & 1 \\
\alpha_1^{2e} & \alpha_2^{2e} & \ldots & \alpha_q^{2e} & 1 & 0
\end{pmatrix}
\]

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

Three-dimensional linear MDS codes of length $q + 2$ are equivalent to *hyperovals* of the finite projective plane.
[MDS Conjecture]

If $4 \leq k \leq q - 2$ then a $k$-dim linear MDS code has length $\leq q + 1$.

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

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

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

$k < q$. $q = p$ [Ball] (2012)

$k < 2\sqrt{q}$. $q = p^2$ [Ball-De Beule] (2012)
If $4 \leq k \leq q - 2$ then a $k$-dim linear MDS code has length $\leq q + 1$.

- $k < \sqrt{q}$. $q$ even [Segre] (1967)
- $k < \sqrt{pq}$. $q = p^{2h+1}$, $q \neq p$ [Voloch] (1991)
- $k < \sqrt{q/2}$. $q = p^{2h}$, $p > 5$ [Hirschfeld-Korchmáros] (1996).
- $k < q$. $q = p$ [Ball] (2012)
- $k < 2\sqrt{q}$. $q = p^2$ [Ball-De Beule] (2012)
- $k < \sqrt{q}$. $q$ odd [Ball-Lavrauw] (2018)
[Lemma] $G$ is the generator matrix of a $k$-dimensional MDS code iff every set of $k$ columns of $G$ is a basis of $\mathbb{F}_q^k$.

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

Equivalently, we can consider $S$ as a set of points in the corresponding projective space.

To prove the MDS conjecture we have to show that if $4 \leq k \leq q - 2$ then $S$ has size at most $q + 1$. 
Let \( A \) be a subset of \( S \) of size \( k - 2 \).

In each of the \( q + 1 \) hyperplanes containing \( A \), there is at most one other vector of \( S \).

(If not then there is a hyperplane containing a set of \( k \) vectors of \( S \) contradicting the arc property.)

So \( |S| \leq k - 2 + q + 1 = q + k - 1 \), or equivalently \( d \leq q \).

For the Reed-Solomon codes \( d \leq q - k \).

There is a possibility that there are MDS codes which are much better than the Reed-Solomon codes.
There are two known examples of linear MDS codes of length $q + 1$ with $4 \leq k \leq q - 2$ which are not Reed-Solomon codes.

[Glynn 1986] $k = 5$, $q = 9$ and $\eta^4 = -1$.

$$G = \begin{pmatrix}
1 & 1 & \ldots & 1 & 0 \\
a_1 & a_2 & \ldots & a_q & 0 \\
a_1^2 + \eta a_1^6 & a_2^2 + \eta a_2^6 & \ldots & a_q^2 + \eta a_q^6 & 0 \\
a_1^3 & a_2^3 & \ldots & a_q^3 & 0 \\
a_1^4 & a_2^4 & \ldots & a_q^4 & 1
\end{pmatrix}$$

[Segre 1967] $k = 4$ or $k = q - 3$, $q = 2^h$ and $(e, h) = 1$.

$$G = \begin{pmatrix}
1 & 1 & \ldots & 1 & 0 \\
a_1 & a_2 & \ldots & a_q & 0 \\
a_1^{2^e} & a_2^{2^e} & \ldots & a_q^{2^e} & 0 \\
a_1^{2^e+1} & a_2^{2^e+1} & \ldots & a_q^{2^e+1} & 1
\end{pmatrix}$$
For every $A \subset S$ of size $k - 2$, there are

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

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

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

The $|S|^{k-2}$ points dual to these hyperplanes lie on an algebraic hypersurface of small degree.
For every $A \subset S$ of size $k - 2$, there are

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

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


The $\binom{|S|}{k-2} t$ points dual to these hyperplanes lie on an algebraic hypersurface of small degree.
For every $A \subset S$ of size $k - 2$, define a polynomial

$$f_A(X) = \prod_{i=1}^{t} \alpha_i(X),$$

the product is over the $t$ linear maps $\alpha_i$ whose kernels are the $t$ hyperplanes containing the vectors of $A$ and no others from $S$.

(Restricting to the case $t$ is odd.)


For any $(k - 3)$-subset $D$ of $S$ and for all $x, y \in S \setminus D$,

$$f_{D \cup \{x\}}(y) = f_{D \cup \{y\}}(x).$$
For any subset $C$ of $S$ of size $k - 1$, there is a $a_C \in \mathbb{F}_q$ such that for all $e \in C$

$$a_C = f_{C \setminus \{e\}}(e).$$

Let $E$ be a subset of $S$ of size $k + t$.

By interpolating the polynomial $f_A(X)$ for each $(k - 2)$-subset $A$ of $E$, we get the equation

$$\sum_C a_C \prod_{u \in E \setminus C} \det(u, C)^{-1} = 0,$$

where the sum is over the $(k - 1)$-subsets $C \subset E$ containing $A$. 
With this system of equations one can prove the following.

[Ball] (2012) If \( k \leq p, \ k \neq (p + 1)/2 \), then a \( k \)-dim linear MDS code of length \( q + 1 \) is a Reed-Solomon code.

[Ball-De Beule] (2012) If \( k \leq 2p − 2 \) then there are no \( k \)-dim linear codes longer than the Reed-Solomon code.

[Ball-De Beule] (2017) A \( k \)-dim linear MDS code of length \( 3k − 6 \) over \( \mathbb{F}_q, \ q \) odd, which can be extended to a Reed-Solomon code, cannot be extended to a linear MDS code of length \( q + 2 \).

[Chowdhury] (2017) conjectures that these equations should be enough to prove the MDS conjecture for \( q \) odd, for nearly all values of \( k \).
Let $S$ be an arc in the projective plane (i.e. its points are the columns of a generator matrix of a 3-dimensional linear MDS code).

There is a $(t, t)$-form $F(X, Y)$ such that

$$F(X, y) = f_y(X)$$

for all $y \in S$.

Therefore, the non-zero coefficients of $X^j$ in

$$F(X + Y, Y) - F(X, Y)$$

are small degree polynomials defining curves containing $S$.
A planar arc of size \( q + 2 - t \), which is not contained in a conic, is contained in the intersection of two curves, which do not share a common component, and have degree at most \( t + p^\lfloor \log_p t \rfloor \).

If \( q \) is odd then an arc of size at least \( q - \sqrt{q} + \sqrt{q/p} + 3 \) is contained in a conic.

This implies that the MDS conjecture is true for \( q \) odd and \( k < \sqrt{q} \).
Are there $k$-dimensional linear MDS codes over $\mathbb{F}_q$ of length $> q + 1$ with $4 \leq k \leq q - 2$ . . .

<table>
<thead>
<tr>
<th>$q$ prime</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q = p^2$</td>
<td>Not in $k &lt; 2\sqrt{q}$ or $k &gt; q - 2\sqrt{q}$.</td>
</tr>
<tr>
<td>$q = p^{2h+1}$</td>
<td>Not in $k &lt; \sqrt{pq}$ or $k &gt; q - \sqrt{pq}$.</td>
</tr>
<tr>
<td>$q$ square</td>
<td>Not in $k &lt; \sqrt{q}$ or $k &gt; q - \sqrt{q}$.</td>
</tr>
</tbody>
</table>

Any $k$-dimensional linear MDS codes over $\mathbb{F}_q$ of length $> (q + k)/2$

would be interesting.