The Maximum Distance Separable (MDS) Codes Conjecture

Jiyou Li
lijiyou@sjtu.edu.cn

Shanghai Jiao Tong University

May 18th, 2013
Outline

1. Introduction
2. Results
3. Ball’s proof according to Ball’s slides
4. MDS codes for AG codes
A Simple Communication Model

Message Source

Source Encoder

Channel

Source Decoder

Receiver
A Simple Communication Model: Example

banana

00

Channel

00

banana
A Simple Communication Model
A Simple Communication Model

banana

00

Channel

apple

01

Noisy!
An Error Correcting Communication Model

- **Message Source**
- **Source Encoder**
- **Channel Encoder**
- **Channel**
- **Channel Decoder**
- **Source Decoder**
- **Receiver**
An Example of Repetition Codes

banana

00

00000

Channel

00001
A photo of Callisto
What is a code (Channel Encoder)

- Let $\mathbf{F}_q$ be the finite field of $q$ elements;
What is a code (Channel Encoder)

- Let $\mathbb{F}_q$ be the finite field of $q$ elements;
- For integers $1 \leq k \leq n$, an $[n, k]_q$ code $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$;

$$C : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n.$$
What is a code (Channel Encoder)

- Let $\mathbf{F}_q$ be the finite field of $q$ elements;
- For integers $1 \leq k \leq n$, an $[n, k]_q$ code $C$ is a $k$-dimension subspace of $\mathbf{F}_q^n$ over $\mathbf{F}_q$;

$$C : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n;$$

- The minimum distance $d(C)$ of $C$ is defined to be the smallest size of the support of a nonzero element in $C$;
What is a code (Channel Encoder)

- Let $\mathbb{F}_q$ be the finite field of $q$ elements;
- For integers $1 \leq k \leq n$, an $[n, k]_q$ code $C$ is a $k$-dimension subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$;

$$C : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n;$$

- The minimum distance $d(C)$ of $C$ is defined to be the smallest size of the support of a nonzero element in $C$;
- $C$ is called an $[n, k, d]_q$ code if $d(C) = d$. 
A code with minimum distance $d$
An Example of Repetition Code

banana

00

000000

Channel

000001

banana

00
Important parameters and MDS codes

- The information rate $\frac{k}{n}$;
Important parameters and MDS codes

- The information rate $\frac{k}{n}$;
- The relative distance $\frac{d}{n}$;

Singleton bound: $k + d \leq 1 + \frac{1}{n}$;

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

Examples: Reed-Solomon Codes
Important parameters and MDS codes

- The information rate \( \frac{k}{n} \);
- The relative distance \( \frac{d}{n} \);
- C is theoretically good if both \( \frac{k}{n} \) and \( \frac{d}{n} \) are large;
Important parameters and MDS codes

- The information rate $\frac{k}{n}$;
- The relative distance $\frac{d}{n}$;
- C is theoretically good if both $\frac{k}{n}$ and $\frac{d}{n}$ are large;
- Singleton bound: $\frac{k}{n} + \frac{d}{n} \leq 1 + \frac{1}{n}$;
Important parameters and MDS codes

- The information rate $\frac{k}{n}$;
- The relative distance $\frac{d}{n}$;
- C is theoretically good if both $\frac{k}{n}$ and $\frac{d}{n}$ are large;
- Singleton bound: $\frac{k}{n} + \frac{d}{n} \leq 1 + \frac{1}{n}$;
- If $d = n - k + 1$, then $C$ is called a maximum distance separable (MDS) code.

Examples: Reed-Solomon Codes
Important parameters and MDS codes

- The information rate $\frac{k}{n}$;
- The relative distance $\frac{d}{n}$;
- $C$ is theoretically good if both $\frac{k}{n}$ and $\frac{d}{n}$ are large;
- Singleton bound: $\frac{k}{n} + \frac{d}{n} \leq 1 + \frac{1}{n}$;
- If $d = n - k + 1$, then $C$ is called a maximum distance separable (MDS) code.
- Examples: Reed-Solomon Codes
Generalized Reed-Solomon codes

- \( D = \{x_1, \cdots, x_n\} \subset F_q, \ |D| = n > 0. \) For \( 1 \leq k \leq n, \) denote by \( D_{n,k} \) the subspace spanned by

\[
(f(x_1), \cdots, f(x_n)) \in F_q^n,
\]

where \( \deg(f(x)) \leq k - 1; \)
Generalized Reed-Solomon codes

1. \( D = \{ x_1, \cdots, x_n \} \subset F_q, \ |D| = n > 0. \) For \( 1 \leq k \leq n, \) denote by \( D_{n,k} \) the subspace spanned by

\[
(f(x_1), \cdots, f(x_n)) \in F_q^n,
\]

where \( \text{deg}(f(x)) \leq k - 1; \)

2. Since a polynomial of degree \( k - 1 \) has at most \( k - 1 \) roots, we have \( d = n - k + 1 \) and thus \( D_{n,k} \) are (MDS) codes.
The followings are all equivalent

- An **MDS** $[n, k, d]$ linear code.
The followings are all equivalent

- An **MDS** \([n, k, d]\) linear code.
- A \(k \times (n - k)\) matrix over \(\mathbb{F}_q\) such that every minor is nonzero.
The followings are all equivalent

- An **MDS** $[n, k, d]$ linear code.
- A $k \times (n - k)$ matrix over $\mathbb{F}_q$ such that every minor is nonzero.
- A set of $n$ vectors in $\mathbb{F}_q^k$ such that any $k$ vectors in $S$ are linearly independent.
The followings are all equivalent

- An **MDS** \([n, k, d]\) linear code.
- A \(k \times (n - k)\) matrix over \(\mathbb{F}_q\) such that every minor is nonzero.
- A set of \(n\) vectors in \(\mathbb{F}_q^k\) such that any \(k\) vectors in \(S\) are linearly independent.
- A set of \(n\) projective points in \(\text{PG}(k - 1, q)\) such that there are at most \(k - 1\) points in any hyperplane of \(\text{PG}(k - 1, q)\).
They are all equivalent

\[
\begin{pmatrix}
1 & 0 & \ldots & 0 & a_{11} & \ldots & a_{1,n-k} \\
0 & 1 & \ldots & 0 & a_{21} & \ldots & a_{2,n-k} \\
0 & 0 & \ldots & 1 & a_{k1} & \ldots & a_{k,n-k}
\end{pmatrix}_{k \times n}
\]
A \([q + 1, k, q - k + 2]_q\) code

\[
\begin{pmatrix}
1 & 1 & \ldots & 1 & 0 \\
a_1 & a_2 & \ldots & a_q & 0 \\
a_1^2 & a_2^2 & \ldots & a_q^2 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_1^{k-1} & a_2^{k-1} & \ldots & a_q^{k-1} & 1
\end{pmatrix}
\]
A $[q + 2, 3, q]_q$ MDS code

- When $q$ is even,

\[
\begin{pmatrix}
1 & 1 & \ldots & 1 & 0 & 0 \\
 a_1 & a_2 & \ldots & a_q & 1 & 0 \\
 a_1^2 & a_2^2 & \ldots & a_q^2 & 0 & 1
\end{pmatrix}.
\]
A \([q + 2, 3, q]_q\) MDS code

- When \(q\) is even,

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 & 0 & 0 \\
\mathbf{a}_1 & \mathbf{a}_2 & \cdots & \mathbf{a}_q & 1 & 0 \\
\mathbf{a}_1^2 & \mathbf{a}_2^2 & \cdots & \mathbf{a}_q^2 & 0 & 1
\end{pmatrix}.
\]

- Question: Why not odd \(q\)?
MDS conjecture

Let $M(k, q)$ be the maximum length $n$ of an $[n, k, n - k + 1]_q$ code;
MDS conjecture

- Let $M(k, q)$ be the maximum length $n$ of an $[n, k, n - k + 1]_q$ code;
- (Bush, 1952) If $k \geq q + 1$, then $M(k, q) = k + 1$. 
Let $M(k, q)$ be the maximum length $n$ of an $[n, k, n - k + 1]_q$ code;

(Bush, 1952) If $k \geq q + 1$, then $M(k, q) = k + 1$.

(Conjectured by Segre, 1955) If $k \leq q$, then $M(k, q) = q + 1$, except the cases that when $q$ is even and $k = 3$ or $k = q - 1$, in which cases $M(k, q) = q + 2$. An easy bound $M(k, q) \leq q + k + 1$. 

MDS conjecture
Let $M(k, q)$ be the maximum length $n$ of an $[n, k, n - k + 1]_q$ code;

(Bush, 1952) If $k \geq q + 1$, then $M(k, q) = k + 1$.

(Conjectured by Segre, 1955) If $k \leq q$, then $M(k, q) = q + 1$,

except the cases that when $q$ is even and $k = 3$ or $k = q - 1$, in which cases $M(k, q) = q + 2$. 
Let $M(k, q)$ be the maximum length $n$ of an $[n, k, n - k + 1]_q$ code;

(Bush, 1952) If $k \geq q + 1$, then $M(k, q) = k + 1$.

(Conjectured by Segre, 1955) If $k \leq q$, then $M(k, q) = q + 1$,

except the cases that when $q$ is even and $k = 3$ or $k = q - 1$, in which cases $M(k, q) = q + 2$.

An easy bound

$$M(k, q) \leq q + k + 1.$$
Three more problems enunciated by Segre, 1955

- Determine the maximal arcs in $PG(k, q)$;
Three more problems enunciated by Segre, 1955

- Determine the maximal arcs in $PG(k, q)$;
- Does every $(q + 1)$-arc be contained in a rational normal curve?
Three more problems enunciated by Segre, 1955

- Determine the maximal arcs in $PG(k, q)$;
- Does every $(q + 1)$-arc be contained in a rational normal curve?
- What are the $n$'s such that every $n$-arc must be contained in a rational normal curve? And how many?
Three more problems enunciated by Segre, 1955

- Determine the maximal arcs in $PG(k, q)$;
- Does every $(q + 1)$-arc be contained in a rational normal curve?
- What are the $n$'s such that every $n$-arc must be contained in a rational normal curve? And how many?
- (Hirschfeld and Thas) Determine the complete arcs in $PG(k, q)$. 
Notations

- $m(k, q)$: the largest size of an arc in $PG(k, q)$;
Notations

- $m(k, q)$: the largest size of an arc in $PG(k, q)$;
- $m'(k, q)$: the second largest size of a complete arc in $PG(k, q)$;
Notations

- $m(k, q)$: the largest size of an arc in $PG(k, q)$;
- $m'(k, q)$: the second largest size of a complete arc in $PG(k, q)$;
- Each arc with size larger than $m'(k, q)$ is contained in an arc of size $m(k, q)$. 

A normal rational curve in $PG(k, q)$ is defined as:

\[ \{(1, t, t_2, \ldots, t_k) \ | \ t \in \mathbb{F}_q\} \cup \{\infty\}. \] 

A normal rational curve of degree 2 is called a conic.
Notations

- $m(k, q)$: the largest size of an arc in $PG(k, q)$;
- $m'(k, q)$: the second largest size of a complete arc in $PG(k, q)$;
- Each arc with size larger than $m'(k, q)$ is contained in an arc of size $m(k, q)$.
- A normal rational curve in $PG(k, q)$ is defined as:
  $$\left\{(1, t, t^2, \ldots, t^k) \mid t \in \mathbb{F}_q\right\} \cup \{\infty\}.$$
**Notations**

- $m(k, q)$: the largest size of an arc in $PG(k, q)$;
- $m'(k, q)$: the second largest size of a complete arc in $PG(k, q)$;
- Each arc with size larger than $m'(k, q)$ is contained in an arc of size $m(k, q)$.
- A normal rational curve in $PG(k, q)$ is defined as:

  $$\left\{(1, t, t^2, \ldots, t^k) \mid t \in F_q\right\} \cup \{\infty\}.$$ 

- A normal rational curve of degree 2 is called a conic.
(Segre, 1967) In $PG(2, q)$, $q$ odd, a $(q + 1)$-arc is a conic.
Preliminary results

- (Segre, 1967) In $PG(2, q)$, $q$ odd, a $(q + 1)$-arc is a conic.
- (Casse and Glynn, 1985) In $PG(4, q)$, $q$ even, a $(q + 1)$-arc is a normal rational curve.
Preliminary results

- (Segre, 1967) In $PG(2, q)$, $q$ odd, a $(q + 1)$-arc is a conic.
- (Casse and Glynn, 1985) In $PG(4, q)$, $q$ even, a $(q + 1)$-arc is a normal rational curve.
- It is elementary that $m(2, q) = q + 1$ if $q$ is odd and otherwise $m(2, q) = q + 2$. 
Preliminary results

- (Segre, 1967) In $\text{PG}(2, q)$, $q$ odd, a $(q + 1)$-arc is a conic.
- (Casse and Glynn, 1985) In $\text{PG}(4, q)$, $q$ even, a $(q + 1)$-arc is a normal rational curve.
- It is elementary that $m(2, q) = q + 1$ if $q$ is odd and otherwise $m(2, q) = q + 2$.
- In $\text{PG}(2, q)$, $q$ even, a $(q + 2)$-arc is a conic plus a nucleus.
Preliminary results

Theorem

(H. Kaneta and T. Maruta, 1989) In $\text{PG}(k, q)$, $q$ odd, $k > 3$. Then

(i). if $\mathcal{K}$ is an $n$-arc with $n > m'(2, q) + k - 2$, then $\mathcal{K}$ lies on a unique normal rational curve;

(ii). If $q + 1 > m'(2, q) + k - 2$, then every $(q + 1)$-arc is a normal rational curve;

(iii). if $q + 1 > m'(2, q) + k - 3$, then $m(k, q) = q + 1$. 
Main results

**Theorem (Segre, 1967; Blokhuis et al., 1990)**

The tangents to an $n$-arc $\mathcal{K}$ in $\text{PG}(2, q)$ belong to an algebraic envelope $F$ of class $t$ or $2t$ according as $q$ is even or odd, where $t = q + 2 - n$. 
Recent Results

- (Segre, 1967) $m'(2, q) = q - \sqrt{q} + 1$ for $q = 2^{2e}, e > 1$. 

Recent Results

- (Segre, 1967) \( m'(2, q) = q - \sqrt{q} + 1 \) for \( q = 2^{2e}, e > 1 \).
- (Segre, 1967) \( m'(2, q) < q - \frac{\sqrt{q}}{4} + \frac{25}{16} \) for \( q \) odd.
Recent Results

- (Segre, 1967) $m'(2, q) = q - \sqrt{q} + 1$ for $q = 2^{2e}, e > 1$.
- (Segre, 1967) $m'(2, q) < q - \frac{\sqrt{q}}{4} + \frac{25}{16}$ for $q$ odd.
- (Voloch, 1990) $m'(2, q) < \frac{44}{45}q + \frac{9}{8}$ for $q$ prime, $q > 5$. 
Recent Results

- (Segre, 1967) \( m'(2, q) = q - \sqrt{q} + 1 \) for \( q = 2^{2e}, e > 1 \).
- (Segre, 1967) \( m'(2, q) < q - \frac{\sqrt{q}}{4} + \frac{25}{16} \) for \( q \) odd.
- (Voloch, 1990) \( m'(2, q) < \frac{44}{45} q + \frac{9}{8} \) for \( q \) prime, \( q > 5 \).
- (Hirschfeld and Korchmáros, 1994) \( m'(2, q) < q - \frac{1}{2} \sqrt{q} + 5 \) for \( q = p^{2h} \) with \( p > 5 \).
Recent Results

- (Segre, 1967) \( m'(2, q) = q - \sqrt{q} + 1 \) for \( q = 2^{2e}, e > 1 \).
- (Segre, 1967) \( m'(2, q) < q - \frac{\sqrt{q}}{4} + \frac{25}{16} \) for \( q \) odd.
- (Voloch, 1990) \( m'(2, q) < \frac{44}{45} q + \frac{9}{8} \) for \( q \) prime, \( q > 5 \).
- (Hirschfeld and Korchmáros, 1994) \( m'(2, q) < q - \frac{1}{2} \sqrt{q} + 5 \) for \( q = p^{2h} \) with \( p > 5 \).
- (Voloch, 1991) \( m'(2, q) < q - \sqrt{2q} + 2 \) for \( q = 2^{2e+1}, e > 1 \).
Recent Results

- (Segre, 1967) $m'(2, q) = q - \sqrt{q} + 1$ for $q = 2^{2e}, e > 1$.
- (Segre, 1967) $m'(2, q) < q - \frac{\sqrt{q}}{4} + \frac{25}{16}$ for $q$ odd.
- (Voloch, 1990) $m'(2, q) < \frac{44}{45}q + \frac{9}{8}$ for $q$ prime, $q > 5$.
- (Hirschfeld and Korchmehros, 1994) $m'(2, q) < q - \frac{1}{2}\sqrt{q} + 5$ for $q = p^{2h}$ with $p > 5$.
- (Voloch, 1991) $m'(2, q) < q - \sqrt{2}q + 2$ for $q = 2^{2e+1}, e > 1$.
- Recall if $n > m'(2, q) + k - 2$ then an $n$-arc is contained in a rational curve. Thus for odd $q$, the MDS conjecture holds when $k - 1$ satisfies above bounds!
Results on MDS conjecture

Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
Results on MDS conjecture

Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
- (Segre, 1967) $k < \frac{\sqrt{q}}{4}$ for $q$ odd;
Results on MDS conjecture

Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
- (Segre, 1967) $k < \frac{\sqrt{q}}{4}$ for $q$ odd;
- (Voloch, 1990) $k < \frac{1}{45} q$ for $q$ prime, $q > 5$;
- (Ball, 2010) $k < q$, $q = p$;
- (Ball, 2011) $k < 2\sqrt{q}$, $q = p^2$. 

Results on MDS conjecture

Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
- (Segre, 1967) $k < \frac{\sqrt{q}}{4}$ for $q$ odd;
- (Voloch, 1990) $k < \frac{1}{45}q$ for $q$ prime, $q > 5$;
- (Hirschfeld and Korchmhros, 1994) $k < \frac{1}{2}\sqrt{q}$ for $q = p^{2h}$ with $p > 5$;
Results on MDS conjecture

Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
- (Segre, 1967) $k < \frac{\sqrt{q}}{4}$ for $q$ odd;
- (Voloch, 1990) $k < \frac{1}{45}q$ for $q$ prime, $q > 5$;
- (Hirschfeld and Korchmhros, 1994) $k < \frac{1}{2}\sqrt{q}$ for $q = p^{2h}$ with $p > 5$;
- (Voloch, 1991) $k < \sqrt{2q}$ for $q = 2^{2e+1}, e > l$;
Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
- (Segre, 1967) $k < \frac{\sqrt{q}}{4}$ for $q$ odd;
- (Voloch, 1990) $k < \frac{1}{45}q$ for $q$ prime, $q > 5$;
- (Hirschfeld and Korchmhoros, 1994) $k < \frac{1}{2}\sqrt{q}$ for $q = p^{2h}$ with $p > 5$;
- (Voloch, 1991) $k < \sqrt{2q}$ for $q = 2^{2e+1}, e > l$;
- (Ball, 2010) $k < q$, $q = p$;
Results on MDS conjecture

Let $M(k, q) = m(k - 1, q)$ be defined as above. Then the main conjecture holds when

- (Segre, 1967) $k < \sqrt{q}$ for $q = 2^{2e}, e > 1$;
- (Segre, 1967) $k < \frac{\sqrt{q}}{4}$ for $q$ odd;
- (Voloch, 1990) $k < \frac{1}{45} q$ for $q$ prime, $q > 5$;
- (Hirschfeld and Korchmáros, 1994) $k < \frac{1}{2} \sqrt{q}$ for $q = p^{2h}$ with $p > 5$;
- (Voloch, 1991) $k < \sqrt{2q}$ for $q = 2^{2e+1}, e > l$;
- (Ball, 2010) $k < q$, $q = p$;
- (Ball, 2011) $k < 2\sqrt{q}$, $q = p^2$. 

Ball’s proof

Please refer to the talk by S. Ball.
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 $S$.


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 $k - 3$,

$$T_{B \cup x}(y) T_{B \cup y}(z) T_{B \cup z}(x) = (-1)^{t+1} T_{B \cup x}(z) T_{B \cup y}(x) T_{B \cup z}(y)$$
\[ s = (s_1, s_2, s_3) \]

\[ s_2 X_1 - s_1 X_2 = 0 \]

\[ a_{13} X_1 + a_{23} X_2 = 0 \]

\[ T_z(X) = \begin{bmatrix} a_{13} X_1 + a_{23} X_2 \end{bmatrix} \]

\[ T_z(x) = \begin{bmatrix} a_{13} \end{bmatrix} \]

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

\[ \frac{s_2}{s_1} \begin{bmatrix} a_{13} \end{bmatrix} (-1)^{t} = -1 \]

\[ T_x(y) T_y(z) = (-1)^{t+1} T_x(y) T_y(z) \]
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 $r = 1, \ldots, \min(p - 1, t + 2)$,

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

where $|L| = r$, $|D| = k - 1 - r$ and $\ell_0$ 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.
AG codes

Let $X/F_q$ be a geometrically irreducible smooth projective curve of genus $g$ over the finite field $F_q$ with function field $F_q(X)$. 
Let $X/F_q$ be a geometrically irreducible smooth projective curve of genus $g$ over the finite field $F_q$ with function field $F_q(X)$.

Let $X(F_q)$ be the set of all $F_q$-rational points on $X$. 
AG codes

- Let $X/F_q$ be a geometrically irreducible smooth projective curve of genus $g$ over the finite field $F_q$ with function field $F_q(X)$.
- Let $X(F_q)$ be the set of all $F_q$-rational points on $X$.
- Let $D = \{P_1, P_2, \ldots, P_n\}$ be a proper subset of rational points $X(F_q)$. 
AG codes

- Let $X/F_q$ be a geometrically irreducible smooth projective curve of genus $g$ over the finite field $F_q$ with function field $F_q(X)$.
- Let $X(F_q)$ be the set of all $F_q$-rational points on $X$.
- Let $D = \{P_1, P_2, \ldots, P_n\}$ be a proper subset of rational points $X(F_q)$.
- Denote $D$ by $D = P_1 + P_2 + \cdots + P_n$. 
Let $X/\mathbb{F}_q$ be a geometrically irreducible smooth projective curve of genus $g$ over the finite field $\mathbb{F}_q$ with function field $\mathbb{F}_q(X)$.

Let $X(\mathbb{F}_q)$ be the set of all $\mathbb{F}_q$-rational points on $X$.

Let $D = \{P_1, P_2, \ldots, P_n\}$ be a proper subset of rational points $X(\mathbb{F}_q)$.

Denote $D$ by $D = P_1 + P_2 + \cdots + P_n$.

Let $G$ be a divisor of degree $m$ ($2g - 2 < m < n$) such that $\text{Supp}(G) \cap D = \emptyset$. 

MDS codes for AG codes
AG codes

- Let $V$ be a divisor.
AG codes

- Let $V$ be a divisor.
- Denote by $\mathcal{L}(V)$ the $\mathbb{F}_q$-vector space of all rational functions $f \in \mathbb{F}_q(X)$ with $\text{div}(f) \geq -V$, together with 0 function.
AG codes

- Let $V$ be a divisor.
- Denote by $\mathcal{L}(V)$ the $\mathbb{F}_q$-vector space of all rational functions $f \in \mathbb{F}_q(X)$ with $\text{div}(f) \geq -V$, together with 0 function.
- The functional AG code $C_L(D, G)$ is defined to be the image of the following evaluation map:

$$ev : \mathcal{L}(V) \rightarrow \mathbb{F}_q^n; f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)).$$
Theorem (Katsman and Tsfasman (1987), Munucra (1992), Walker (1996))

*The MDS conjecture for elliptical curves holds.*
AG codes for curves

- \( d(C_L(D, G)) \geq n - m \) and \( m = \text{deg}(G) \).
AG codes for curves

- \( d(C_L(D, G)) \geq n - m \) and \( m = \text{deg}(G) \).
- By Riemann-Roch theorem, the AG code \( C_L(D, G) \) has parameters \([n, m - g + 1, d \geq n - m]\).
AG codes for curves

- \( d(C_L(D, G)) \geq n - m \) and \( m = \text{deg}(G) \).
- By Riemann-Roch theorem, the AG code \( C_L(D, G) \) has parameters \([n, m - g + 1, d \geq n - m]\).
- By the Singleton bound, we have

\[
  n - m \leq d \leq n - m + g.
\]
AG codes for curves

- $d(C_L(D, G)) \geq n - m$ and $m = \text{deg}(G)$.
- By Riemann-Roch theorem, the AG code $C_L(D, G)$ has parameters $[n, m - g + 1, d \geq n - m]$.
- By the Singleton bound, we have

$$n - m \leq d \leq n - m + g.$$

- When $g = 1$ one has

$$n - m \leq d \leq n - m + 1.$$
To determine the minimum distance of a code

- When $g = 1$ one has a $[n, n - m, d]$ code with
  
  $$n - m \leq d \leq n - m + 1.$$
To determine the minimum distance of a code

- When \( g = 1 \) one has a \([n, n - m, d]\) code with
  \[
  n - m \leq d \leq n - m + 1 .
  \]

- In general, Cheng showed that determining \( d \) exactly is an \textbf{NP}-complete problem.
SSP in the Mordell group of an elliptical curve

**Theorem (Q. Cheng, 2005)**

\[ d = n - m \text{ if and only if a suitable subset sum has a solution.} \]
The proof

\[ E(\mathbb{F}_q) \cong \text{div}^0(E)/\text{Prin}(\mathbb{F}_q(E)) \]
The proof

- \( E(\mathbb{F}_q) \cong \text{div}^0(E) / \text{Prin}(\mathbb{F}_q(E)) \)

- \[ N_G(k, b, D) = \# \{ S \subseteq D | \# S = k \text{ and } \sum_{x \in S} x = b \} . \]
The proof

- $E(\mathbb{F}_q) \cong \text{div}^0(E)/\text{Prin}(\mathbb{F}_q(E))$

- $N_G(k, b, D) = \#\left\{ S \subseteq D \mid \#S = k \text{ and } \sum_{x \in S} x = b \right\}.$

- Let $G = (m - 1)0 + P$ ($0 < m < n$). Endow $E(\mathbb{F}_q)$ a group structure with the zero element $O$. 

\[ N_G(k, b, D) = \#\left\{ S \subseteq D \mid \#S = k \text{ and } \sum_{x \in S} x = b \right\}. \]
The proof

- \( E(\mathbb{F}_q) \cong \text{div}^0(E)/\text{Prin}(\mathbb{F}_q(E)) \)

\[
N_G(k, b, D) = \# \{ S \subseteq D \mid \# S = k \text{ and } \sum_{x \in S} x = b \}.
\]

- Let \( G = (m - 1)0 + P \) (\( 0 < m < n \)). Endow \( E(\mathbb{F}_q) \) a group structure with the zero element \( O \).

- Then the AG code \( C_L(D, G) \) is an MDS code, i.e., \( d = n - m + 1 \) if and only if

\[
N(m, P, D) = 0.
\]
A counting proof of the MDS conjecture for elliptical curves

**Theorem (with D. Wan and J. Zhang, 2013)**

*The MDS conjecture for elliptical curves holds.*
Thank you very much for your attention!