The maximum weight of a linear code

Simeon Ball
A linear code $C$ over $\mathbb{F}_q$ of length $n$, dimension $k$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$.

The weight of a vector is the number of non-zero coordinates.

Let $d$ denote the minimum weight and let $m$ denote the maximum weight of a vector of $C$.

The distance between any two vectors is the number of coordinates in which they differ. The minimum distance of a linear code is $d$. 
If $q$ is prime then

$$m \leq (n - d - e)q + e,$$

where $e \leq k - 2$ is maximal with the property that

$$\binom{n-d}{e} \neq 0 \pmod{q^{k-1-e}}.$$
There is a 3-dimensional linear code over $\mathbb{F}_{13}$ of length 145 and minimum distance 133.

The bound $m \leq (n - d - e)q + e$ gives

$$m \leq 11 \times 13 + 1 = 144$$

so this code has no codeword of weight 145.
[Ball-Blokhuis 2012] If $q$ is prime and $C$ contains a codeword of weight $n$ then

$$n \geq d + e + d/(q - 1),$$

where $e \leq k - 2$ is maximal with the property that

$$\binom{n - d}{e} \not\equiv 0 \pmod{q^{k-1-e}}.$$
This bound \( n \geq d + e + d/(q - 1) \) is attained by many codes. For example it implies that,

a binary code of minimum distance 7 and dimension 12 has length at least 23,  
(binary Golay code)  
a ternary code of minimum distance 6 and dimension 6 has length at least 12.  
(extended ternary Golay code)
The bound

\[ n \geq d + e + d/(q - 1) \]

improves on the Griesmer bound

\[ n \geq d + \left\lfloor \frac{d}{q} \right\rfloor + \left\lfloor \frac{d}{q^2} \right\rfloor + \ldots + \left\lfloor \frac{d}{q^{k-1}} \right\rfloor. \]

by \( (d_r + d_{r+1} + \ldots + d_{k-2})/(q - 1) + e - k + 1 + r, \)
where \( d = d_r q^r + d_{r+1} q^{r+1} + d_{r+2} q^{r+2} + \ldots + d_{k-2} q^{k-2}. \)
We want to prove the bound $m \leq (n - d - e)q + e$.

If $m \leq n - d$ then the Singleton bound $(n - d \geq k - 1)$ and $k - 2 \geq e$ imply the bound.

If $m \geq n - d + 1$ then the code $C$ shortens to a code of length $m$, dimension $k$ and minimum distance at least $d - (n - m)$ containing a codeword of weight $m$. 
Let $G$ be a generator matrix of a linear code $C$, so

$$C = \{ (x_1, \ldots, x_k)G \mid (x_1, \ldots, x_k) \in \mathbb{F}_q^k \}.$$ 

Let $S$ be a set of columns of $G$, considered as points of $\text{PG}(k-1, q)$.

A vector of $C$ has at most $n - d$ zero coordinates, so every hyperplane contains at most $n - d$ points of $S$.

If $C$ contains a codeword of length $n$ then $S$ is contained in $\text{AG}(k-1, q)$. 
A set $S$ of points of $\text{PG}(k-1, q)$ is called a $(n, r)$-arc if $|S| = n$ and $r$ is the max size of the intersections of $S$ with hyperplanes.

(trivial bound for $\text{PG}(k-1, q)$) $n \leq (r - k + 2)q + r$

(trivial bound for $\text{AG}(k-1, q)$) $n \leq rq$

and we want to prove the bound $n \leq (r - e)q + e$, where $e \leq k - 2$ is maximal with the property that

$$\binom{r}{e} \not\equiv 0 \pmod{q^{k-1-e}}.$$
Bounds for $\text{AG}(k-1, q)$, where $q = p^h$ and $r < q^{k-2}$.

[Barlotti 1956]
If $k = 3$ and $(r, q) = 1$ then $n \leq (r - k + 2)q + r - 2$.

[Lunelli-Sce 1964]
If $k = 3$ and $(r, q) = 1$ then $n \leq (r - k + 2)q + r - 3$.

[Bruen 1992]
$n \leq (r - k + 2)q + q^{k-2} - r + k - 3$.

[Lunelli-Sce Conjecture 1964 - Blokhuis 1994]
If $k = 3$ then $n \leq (r - k + 2)q + (r, q)$. 
Bounds for $AG(k - 1, q)$, where $q = p^h$.

[Ball 2000]
If $q^{k-2} > r > q^{k-2} - q$ then $n \leq (r - k + 2)q + k - 2$, provided that
\[
\binom{r}{k-2} \neq 0 \pmod{p}.
\]

[Ball-Blokhuis 2012]
If $q$ is prime then $n \leq (r - e)q + e$,
where $e \leq k - 2$ is maximal with the property that
\[
\binom{r}{e} \neq 0 \pmod{q^{k-1-e}}.
\]
Let $S$ be a set of points of $AG(k - 1, q)$.

Define the Rédei polynomial (over a finite field) of $S$ to be

$$f(T, x_1, \ldots, x_{k-1}) = \prod_{s \in S} (T + x_1 s_1 + \ldots + x_{k-1} s_{k-1}).$$

$T + a$ is a factor of $f(T, x)$ of multiplicity $t$ iff the hyperplane defined by $x_1 X_1 + \ldots + x_{k-1} X_{k-1} = a$ contains $t$ points of $S$. 
Now write

\[ f(T, x_1, \ldots, x_{k-1}) = \prod_{s \in S} (T + x_1 s_1 + \ldots + x_{k-1} s_{k-1}), \]

as a sum

\[ f(T, x_1, \ldots, x_{k-1}) = \sum T^j \sigma_j(x). \]

Advantage: The polynomials \( \sigma_j(x) \) have degree at most \( |S| - j \).

Disadvantage: Since we are working over a finite field of characteristic \( p \) say, if something is zero it is zero modulo \( p \).
Let $S$ be a set of points of $\text{AG}(k - 1, q)$, $q$ prime.

Define the Rédei polynomial (over $\mathbb{C}$) of $S$ to be

$$f(T, x_1, \ldots, x_{k-1}) = \prod_{s \in S} (T + \eta^{x_1s_1 + \cdots + x_{k-1}s_{k-1}}),$$

where $\eta$ is a primitive $q$-th root of unity.

$T + \eta^a$ is a factor of $f(T, x)$ of multiplicity $t$ iff the hyperplane defined by $x_1X_1 + \cdots + x_{k-1}X_{k-1} = a$ contains $t$ points of $S$. 
Now write

\[ f(T, x_1, \ldots, x_{k-1}) = \prod_{s \in S} (T + \eta^{x_1s_1 + \cdots + x_{k-1}s_{k-1}}), \]

as a sum

\[ f(T, x_1, \ldots, x_{k-1}) = \sum T^j \sigma_j(x). \]

Advantage: The characteristic of \( \mathbb{C} \) is zero.

Disadvantage: The functions \( \sigma_j(x) \) are not polynomials, but they are integer sums of characters of the additive group of \( \mathbb{F}_q^{k-1} \).
Let $S$ be a set of points of $\text{AG}(k - 1, q)$, $q$ prime, with at most $r$ points on a hyperplane.

$$f(T, x) \text{ divides } (T^q + 1)^r,$$

for all $x = (x_1, \ldots, x_{k-1}) \neq 0$.

This implies that there are functions $g(x)$ which are the integer sum of characters with the property

$$g(x) = 0,$$

for all $x \neq 0$.  

If $g(x)$ is the integer sum of characters with the property

$$g(x) = 0,$$

for all $x \neq 0$, then

$$q^{k-1} \text{ divides } g(0).$$

Moreover, $g(0)$ is a coefficient of

$$(T + 1)^{-|S|}(T^q + 1)^r$$

So, it remains to show that if $|S|$ is too small then this coefficient, which is the sum of binomial coefficients, is not divisible by $q^{k-1}$. 
1. If $q = p^h$ then we should replace $\eta^{x_1s_1+\cdots+x_{k-1}s_{k-1}}$ by $\eta^{Tr(x_1s_1+\cdots+x_{k-1}s_{k-1})}$, where $Tr$ is the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$.

2. The complex Rédei polynomial of any affine set of points with a regularity property may give new information.

3. How should we define the complex Rédei polynomial of a projective set of points with a regularity property?
Let $\mathbb{Z}_p$ denote the $p$-adic integers and $\epsilon$ a prim. root of $X^{q-1} - 1$.

Lift an element $x \in \mathbb{F}_q$ to $\tau(x) \in \mathbb{Z}_p(\epsilon)$, so $\tau(x) = x \mod p$.

Let $S$ be a set of points of $AG(k-1, q)$.

Define the Rédei polynomial (over $\mathbb{Z}_p(\epsilon)$) of $S$ to be

$$f(T, x_1, \ldots, x_{k-1}) = \prod_{s \in S} (T + x_1 \tau(s_1) + \ldots + x_{k-1} \tau(s_{k-1})).$$

$$f(a, x) = 0 \pmod{p^t}$$ if and only if the hyperplane defined by equation $x_1 X_1 + \ldots + x_{k-1} X_{k-1} = a$ contains $t$ points of $S$. 
Now write

\[ f(T, x_1, \ldots, x_{k-1}) = \prod_{s \in S} (T + x_1 s_1 + \ldots + x_{k-1} s_{k-1}), \]

as a sum

\[ f(T, x_1, \ldots, x_{k-1}) = \sum T^j \sigma_j(x). \]

**Advantage:** The \( \sigma_j(x) \) are polynomials.

**Advantage:** The characteristic of \( \mathbb{Z}_p \) is zero.
Suppose that $A$ is a subset of $\mathbb{Z}_p(\epsilon)[X]$ whose elements are pairwise distinct modulo $p$.

To apply the geometric property of $S$ to $f$ we apply the following.

If $f \in \mathbb{Z}_p(\epsilon)[T]$ has the property that that each $a \in A$ there are $m$ factors of $f$ of the type $T + \bar{a}$, where $a = \bar{a} \mod p$ then

$$f(T) = \sum_{j=0}^{m} p^{m-j} g(T)^j$$

where $g(T) = \prod_{a \in A} (T - a)$. 