Asymptotically good codes with asymptotically good squares

Hugues Randriambololona

Telecom ParisTech

DIAMANT Symposium
2012.11.30
Definitions

Let \( \ast \) denote coordinatewise multiplication in \((\mathbb{F}_q)^n\):

\[
(x_1, \ldots, x_n) \ast (y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n).
\]
**Definitions**

Let $\ast$ denote coordinatewise multiplication in $(\mathbb{F}_q)^n$:

$$(x_1, \ldots, x_n) \ast (y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n).$$

If $C \subset (\mathbb{F}_q)^n$ is a $k$-dimensional linear subspace, i.e. an $[n, k]_q$-code, let

$$C \ast C = \{c \ast c' \mid c, c' \in C\} \subset (\mathbb{F}_q)^n$$

and then ("square" of $C$):

$$C \langle 2 \rangle = \langle C \ast C \rangle = \{\sum_{c, c' \in C} \alpha c, c' \ast c' \mid \alpha c, c' \in \mathbb{F}_q\}$$

is the linear span of $C \ast C$.

More generally (higher powers):

$$C \langle t+1 \rangle = \langle C \langle t \rangle \ast C \rangle.$$
Definitions

Let $*$ denote coordinatewise multiplication in $(\mathbb{F}_q)^n$:

$$(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

If $C \subset (\mathbb{F}_q)^n$ is a $k$-dimensional linear subspace, i.e. an $[n, k]_q$-code, let

$$C * C = \{c * c' \mid c, c' \in C\} \subset (\mathbb{F}_q)^n$$

and then ("square" of $C$):

$$C^{(2)} = \langle C * C \rangle = \left\{ \sum_{c, c' \in C} \alpha_{c, c'} c * c' \mid \alpha_{c, c'} \in \mathbb{F}_q \right\}$$

is the linear span of $C * C$. 

Definitions

Let \(*\) denote coordinatewise multiplication in \((\mathbb{F}_q)^n\):

\[(x_1, \ldots, x_n) \ast (y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n)\].

If \(C \subset (\mathbb{F}_q)^n\) is a \(k\)-dimensional linear subspace, i.e. an \([n, k]_q\)-code, let

\[C \ast C = \{ c \ast c' \mid c, c' \in C \} \subset (\mathbb{F}_q)^n\]

and then ("square" of \(C\)):

\[C^{(2)} = \langle C \ast C \rangle = \{ \sum_{c, c' \in C} \alpha_{c, c'} c \ast c' \mid \alpha_{c, c'} \in \mathbb{F}_q \}\]

is the linear span of \(C \ast C\). More generally (higher powers):

\[C^{(t+1)} = \langle C^{(t)} \ast C \rangle\].

Geometric interpretation: Veronese embedding.
A possible motivation

Start from a symmetric bilinear form $B$

$$V \times V \overset{B}{\longrightarrow} W$$
**A possible motivation**

Start from a symmetric bilinear form $B$ and a diagram

\[
\begin{array}{ccc}
V \times V & \xrightarrow{B} & W \\
\phi \times \phi & \downarrow & \theta \\
(\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n
\end{array}
\]

so $B(u, v) = \theta(\phi(u) \ast \phi(v))$ for $u, v \in V$. 
A possible motivation

Start from a symmetric bilinear form $B$ and a diagram

$$
\begin{array}{ccc}
V \times V & \xrightarrow{B} & W \\
\phi \times \phi \downarrow & & \uparrow \theta \\
(F_q)^n \times (F_q)^n & \xrightarrow{*} & (F_q)^n
\end{array}
$$

so $B(u, v) = \theta(\phi(u) \ast \phi(v))$ for $u, v \in V$. More generally

$$
\sum_i B(u^{(i)}, v^{(i)}) = \theta(\sum_i \phi(u^{(i)}) \ast \phi(v^{(i)})) \in \theta(C^{(2)})
$$

where $C = \text{im}(\phi)$. 
A possible motivation

Start from a symmetric bilinear form $B$ and a diagram

\[
\begin{array}{ccc}
V \times V & \xrightarrow{B} & W \\
\phi \times \phi \downarrow & & \uparrow \theta \\
(F_q)^n \times (F_q)^n & \xrightarrow{*} & (F_q)^n \\
\end{array}
\]

so $B(u, v) = \theta(\phi(u) \ast \phi(v))$ for $u, v \in V$. More generally

\[
\sum_i B(u^{(i)}, v^{(i)}) = \theta(\sum_i \phi(u^{(i)}) \ast \phi(v^{(i)})) \in \theta(C^{(2)})
\]

where $C = \text{im}(\phi)$.

Occurs in various contexts:

- algebraic complexity theory
- multi-party computation.
Most often $V = W = \mathbb{F}_{q^r}$ and $B$ is field multiplication. We say $(\phi, \theta)$ define a (symmetric) multiplication algorithm of length $n$ for $\mathbb{F}_{q^r}$.
Most often $V = W = \mathbb{F}_{q^r}$ and $B$ is field multiplication. We say $(\phi, \theta)$ define a (symmetric) multiplication algorithm of length $n$ for $\mathbb{F}_{q^r}$.

Example: multiplication in $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$

$$(x + y\alpha)(x' + y'\alpha) =$$
Most often $V = W = \mathbb{F}_{q^r}$ and $B$ is field multiplication. We say $(\phi, \theta)$ define a (symmetric) multiplication algorithm of length $n$ for $\mathbb{F}_{q^r}$.

Example: multiplication in $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ with $4 \cdot$ in $\mathbb{F}_q$.

$$(x + y\alpha)(x' + y'\alpha) = x \cdot x' + (x \cdot y' + x' \cdot y) \cdot \alpha + y \cdot y' \cdot \alpha^2$$ (note: non-symmetric)
Most often $V = W = \mathbb{F}_{q^r}$ and $B$ is field multiplication. We say $(\phi, \theta)$ define a (symmetric) multiplication algorithm of length $n$ for $\mathbb{F}_{q^r}$.

Example: multiplication in $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ with $3 \cdot$ in $\mathbb{F}_q$

$$(x + y\alpha)(x' + y'\alpha) = x \cdot x' \cdot (1 - \alpha) + (x + y) \cdot (x' + y') \cdot \alpha + y \cdot y' \cdot (\alpha^2 - \alpha)$$

(Karatsuba; geometric interpretation: evaluate at $0, 1, \infty$).
Most often $V = W = \mathbb{F}_{q^r}$ and $B$ is field multiplication. We say $(\phi, \theta)$ define a (symmetric) multiplication algorithm of length $n$ for $\mathbb{F}_{q^r}$.

Example: multiplication in $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ with $3 \cdot$ in $\mathbb{F}_q$

$$(x + y\alpha)(x' + y'\alpha) = x \cdot x' \cdot (1 - \alpha) + (x + y) \cdot (x' + y') \cdot \alpha + y \cdot y' \cdot (\alpha^2 - \alpha)$$

(Karatsuba; geometric interpretation: evaluate at $0, 1, \infty$).

Could work more generally with symmetric $t$-linear maps.

Might then ask for:

- resistance to noise (random errors)
- resistance to malicious users (passive or active)
- threshold properties.

All these are governed essentially by the minimum distance of $C^{(t)}$. 

Hugues Randriam – Asymptotically good codes & their squares
Parameters:

- dimension $\dim \langle t \rangle (C) = \dim (C \langle t \rangle)$
- rate $R \langle t \rangle (C) = R (C \langle t \rangle)$
- minimum distance $d_{\min} \langle t \rangle (C) = d_{\min} (C \langle t \rangle)$
- relative distance $\delta \langle t \rangle (C) = \delta (C \langle t \rangle)$.
Parameters:

- dimension $\dim^{(t)}(C) = \dim(C^{(t)})$
- rate $R^{(t)}(C) = R(C^{(t)})$
- minimum distance $d_{\min}^{(t)}(C) = d_{\min}(C^{(t)})$
- relative distance $\delta^{(t)}(C) = \delta(C^{(t)})$.

For some given $q$, we would like to construct $C$ such that all these parameters up to a certain order $t$ are large. We are interested in the asymptotic case $n \to \infty$. For $q = 2$, already $t = 2$ is non-trivial.
Parameters:

- dimension \( \dim^{(t)}(C') = \dim(C'^{(t)}) \)
- rate \( R^{(t)}(C') = R(C'^{(t)}) \)
- minimum distance \( d_{\min}^{(t)}(C') = d_{\min}(C'^{(t)}) \)
- relative distance \( \delta^{(t)}(C') = \delta(C'^{(t)}) \).

For some given \( q \), we would like to construct \( C' \) such that all these parameters up to a certain order \( t \) are large. We are interested in the asymptotic case \( n \to \infty \). For \( q = 2 \), already \( t = 2 \) is non-trivial.

Easy to show:

**Proposition**

\[
\dim^{(t+1)}(C') \geq \dim^{(t)}(C)
\]
\[
d_{\min}^{(t+1)}(C') \leq d_{\min}^{(t)}(C)
\]

Hence: suffices to give lower bounds on \( \dim(C') \) and \( d_{\min}^{(t)}(C') \) (or on \( R(C') \) and \( \delta^{(t)}(C') \)).
Generalize the fundamental functions of block coding theory:

\[ a_q^{(t)}(n, d) = \max\{ k \geq 0 \mid \exists C \subset (\mathbb{F}_q)^n, \dim(C) = k, d_{\min}^{(t)}(C) \geq d \} \]
Generalize the fundamental functions of block coding theory:

\[
a_q^{\langle t \rangle}(n, d) = \max\{ k \geq 0 \mid \exists C \subset (\mathbb{F}_q)^n, \dim(C) = k, d_{\text{min}}^{\langle t \rangle}(C) \geq d \}
\]

\[
\alpha_q^{\langle t \rangle}(\delta) = \limsup_{n \to \infty} \frac{a_q^{\langle t \rangle}(n, \lfloor \delta n \rfloor)}{n}
\]
Generalize the fundamental functions of block coding theory:

\[ a_q^{(t)}(n, d) = \max \{ k \geq 0 \mid \exists C \subset (\mathbb{F}_q)^n, \dim(C) = k, d_{\min}(C) \geq d \} \]

\[ \alpha_q^{(t)}(\delta) = \limsup_{n \to \infty} \frac{a_q^{(t)}(n, \lfloor \delta n \rfloor)}{n} \]

and then:

\[ \tau(q) = \sup \{ t \in \mathbb{N} \mid \alpha_q^{(t)} \neq 0 \} \]

the supremum value (possibly +\infty?) of \( t \) such that there are asymptotically good codes \( C_i \) over \( \mathbb{F}_q \) whose \( t \)-th powers \( C_i^{(t)} \) are also asymptotically good:

\[ \liminf_i R(C_i) > 0 \quad \text{and} \quad \liminf_i \delta^{(t)}(C_i) > 0. \]
**Theorem 0**

\[ \alpha_q^{(t)}(\delta) \geq \frac{1 - \delta}{t} - \frac{1}{A(q)} \]

hence

\[ \tau(q) \geq \lceil A(q) \rceil - 1 \]

where \( A(q) \) is the **Ihara function** that governs the asymptotic number of points on curves over \( \mathbb{F}_q \).
Results

Theorem 0

\[ \alpha_q^{(t)}(\delta) \geq \frac{1 - \delta}{t} - \frac{1}{A(q)} \]

hence

\[ \tau(q) \geq \lceil A(q) \rceil - 1 \]

where \( A(q) \) is the Ihara function that governs the asymptotic number of points on curves over \( \mathbb{F}_q \).

Theorem 1

\[ \alpha_2^{(2)}(\delta) \geq \frac{74}{39525} - \frac{9}{17} \delta \approx 0.001872 - 0.5294 \delta \]

hence

\[ \tau(2) \geq 2 \]

(and more generally \( \tau(q) \geq 2 \) for all \( q \)).
Proof of Theorem 0 (quite standard)

X curve of genus g over $\mathbb{F}_q$ with n points $P_1, \ldots, P_n$, $G = P_1 + \cdots + P_n$, $D$ disjoint from $G$, $L(D)$ space of functions on $X$ with poles at most $D$, $l(D) = \dim L(D)$,

$$C(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(D)\}.$$
Proof of Theorem 0 (quite standard)

Let $X$ be a curve of genus $g$ over $\mathbb{F}_q$ with $n$ points $P_1, \ldots, P_n$, $G = P_1 + \cdots + P_n$, $D$ disjoint from $G$, $L(D)$ the space of functions on $X$ with poles at most $D$, $l(D) = \dim L(D)$,

$$C(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(D)\}.$$

**Lemma**

$$C(D, G)^{\langle t \rangle} \subset C(tD, G).$$
**Proof of Theorem 0 (quite standard)**

Let $X$ be a curve of genus $g$ over $\mathbb{F}_q$ with $n$ points $P_1, \ldots, P_n$, $G = P_1 + \cdots + P_n$, $D$ disjoint from $G$, $L(D)$ space of functions on $X$ with poles at most $D$, $l(D) = \dim L(D)$,

$$C(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(D)\}.$$

**Lemma**

$$C(D, G)^{\langle t \rangle} \subset C(tD, G).$$

**Lemma (Goppa)**

Suppose $g \leq \deg(D) < n$. Then

$$\dim C(D, G) = l(D) \geq \deg(D) + 1 - g$$

$$d_{\min}(C(D, G)) \geq n - \deg(D).$$
Concatenation

$C$ an $[n, k]$-code over $\mathbb{F}_{q^r}$, $\phi : \mathbb{F}_{q^r} \rightarrow (\mathbb{F}_q)^m$ an injective $\mathbb{F}_q$-linear map, define $\phi(C) = \{ \phi(c) = (\phi(c_1), \ldots, \phi(c_n)) \mid c = (c_1, \ldots, c_n) \in C \}$. Then $\phi(C)$ is an $[mn, kr]$-code over $\mathbb{F}_q$ (identify $((\mathbb{F}_q)^m)^n = (\mathbb{F}_q)^{mn}$).

Other terminology: the outer code is $C_{out} = C$, the inner code is $C_{in} = \text{im}(\phi) \subset (\mathbb{F}_q)^m$, the concatenated code is $C_{out} \circ \phi C_{in} = \phi(C)$.

Strategy: use Theorem 0 over an extension field $\mathbb{F}_{q^r}$, then concatenate to get Theorem 1 over $\mathbb{F}_q$. 
**Concatenation**

$C$ an $[n, k]$-code over $\mathbb{F}_{q^r}$, $\phi : \mathbb{F}_{q^r} \rightarrow (\mathbb{F}_q)^m$ an injective $\mathbb{F}_q$-linear map, define $\phi(C) = \{ \phi(c) = (\phi(c_1), \ldots, \phi(c_n)) \mid c = (c_1, \ldots, c_n) \in C \}$. Then $\phi(C)$ is an $[mn, kr]$-code over $\mathbb{F}_q$ (identify $((\mathbb{F}_q)^m)^n = (\mathbb{F}_q)^{mn}$).

Other terminology: the outer code is $C_{\text{out}} = C$, the inner code is $C_{\text{in}} = \text{im}(\phi) \subset (\mathbb{F}_q)^m$, the concatenated code is $C_{\text{out}} \circ \phi C_{\text{in}} = \phi(C)$.

Strategy: use Theorem 0 over an extension field $\mathbb{F}_{q^r}$, then concatenate to get Theorem 1 over $\mathbb{F}_q$.

Example: a related problem? $C$ is $\varepsilon$-$\cap$ if

$$c_1, c_2 \in C \setminus \{0\} \implies \text{wt}(c_1 * c_2) \geq \varepsilon n.$$  

Easy:

$$C_{\text{out}} \varepsilon$-$\cap$ & $C_{\text{in}} \varepsilon'$$-$\cap$ $\implies$ $C_{\text{out}} \circ C_{\text{in}}$ is $\varepsilon \varepsilon'$-$\cap$.

Same flavour but no logical connection between $C$ $\varepsilon$-$\cap$ and $\delta^{(2)}(C) \geq \varepsilon$.  

Hugues Randriam – Asymptotically good codes & their squares  
DIAMANT Symposium – 2012.11.30
Start with $C$ over $\mathbb{F}_{q^r}$ with control on $d_{\text{min}}^{(2)}(C)$, concatenate with $\phi : \mathbb{F}_{q^r} \longrightarrow (\mathbb{F}_q)^m$, how can we control $d_{\text{min}}^{(2)}(\phi(C))$?

\[
\begin{align*}
C \times C & \longrightarrow C^{(2)} \\
\phi \times \phi & \\
\phi(C) \times \phi(C) & \longrightarrow \phi(C)^{(2)}
\end{align*}
\]
Start with $C$ over $\mathbb{F}_{q^r}$ with control on $d_{\min}^{(2)}(C)$, concatenate with $\phi: \mathbb{F}_{q^r} \longrightarrow (\mathbb{F}_q)^m$, how can we control $d_{\min}^{(2)}(\phi(C))$?

$$
\begin{array}{ccc}
C \times C & \longrightarrow & C^{(2)} \\
\phi \times \phi & \downarrow & \uparrow \theta \\
\phi(C') \times \phi(C') & \longrightarrow & \phi(C')^{(2)}
\end{array}
$$

A smart move is to take $\phi$ from a multiplication algorithm:

$$
\begin{array}{ccc}
\mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \longrightarrow & \mathbb{F}_{q^r} \\
\phi \times \phi & \downarrow & \uparrow \theta \\
(\mathbb{F}_q)^m \times (\mathbb{F}_q)^m & \longrightarrow & (\mathbb{F}_q)^m
\end{array}
$$

and deduce $d_{\min}^{(2)}(\phi(C')) \geq d_{\min}^{(2)}(C)$. 
Unfortunately, this fails...
Unfortunately, this fails...

... the obstruction is $\ker(\theta)$. 
Some preliminary remarks

Suppose there exists a \( \phi : \mathbb{F}_{q^r} \rightarrow (\mathbb{F}_q)^m \) such that for all \( C \) over \( \mathbb{F}_{q^r} \),

\[
\delta^{(2)}(\phi(C)) \geq \kappa \delta^{(2)}(C).
\]

Write \( \phi = (\phi_1, \ldots, \phi_m) \) so the \( \phi_i \) are the columns of the generating matrix of the inner code. Take \( m' \geq m \) and put some more columns in to get \( \phi' : \mathbb{F}_{q^r} \rightarrow (\mathbb{F}_q)^{m'} \). Then we still have

\[
\delta^{(2)}(\phi'(C)) \geq \kappa' \delta^{(2)}(C)
\]

with \( \kappa' = \frac{m}{m'} \kappa \), since \( \phi'(C) \) is an extension of \( \phi(C) \).

The longer \( \phi \), the more chances we have (if any) to prove such a bound.

Extreme example: \( m = \frac{q^r-1}{q-1} \), \( \phi = \) all linear forms, \( C_{in} = \) simplex code.
Also, the longer $\phi$, the easier to find a $\theta$: indeed $\theta$ exists iff multiplication in $\mathbb{F}_{q^r}$ factors through $\Phi = (\phi_1 \otimes 2, \ldots, \phi_r \otimes 2)$.

\[
\begin{array}{ccc}
\mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \longrightarrow & \mathbb{F}_{q^r} \\
\phi \times \phi \downarrow & & \uparrow \theta \\
(\mathbb{F}_q)^m \times (\mathbb{F}_q)^m & \longrightarrow & (\mathbb{F}_q)^m
\end{array}
\]

Recall, if $\lambda$ is a linear form, $\lambda \otimes 2$ is the symmetric bilinear form

\[(v, w) \mapsto \lambda(v)\lambda(w)\]

(or in terms of matrices it is $\lambda \lambda^T$).
On the other hand, perhaps we should not take $\phi$ too long. In particular we could avoid linear dependencies between the $\phi_i \otimes_2$. Indeed:

- If we extend $\phi$ by adding some $\phi_{m+1}$ to it such that $\phi_m \otimes_2$ is linearly dependent on the other $\phi_i \otimes_2$, then we extend $\phi(C')$ by adding a new coordinate in each block, so that in the squared code, these new coordinates are linearly dependent on the others. So if a codeword in $\phi(C')^{\langle 2 \rangle}$ is zero on some block, it is still zero on this block after extending.

- Linear relations between the $\phi_i \otimes_2$ make the choice of $\theta$ non-unique, hence non-canonical. We want to understand the structure of $\ker(\theta)$. Most often, canonical objects have a more interesting structure than non-canonical ones.
The symmetric square of a space

Let \( V \) be a vector space over \( \mathbb{F}_q \). Recall:

\[
S^2_{\mathbb{F}_q} V = \langle u \cdot v \rangle_{u,v \in V} / \text{(sym. bilin. rel.)}
\]
\[
= V \otimes V / \langle u \otimes v - v \otimes u \rangle_{u,v \in V}
\]
\[
= \text{Sym}(V; \mathbb{F}_q) \vee.
\]

In the last identification, \( u \cdot v \) is \( \text{Sym}(V; \mathbb{F}_q) \to \mathbb{F}_q, \psi \mapsto \psi(u,v) \).

Every symmetric bilinear map \( B : V \times V \to W \) factorizes uniquely as

\[
V \times V \to S^2_{\mathbb{F}_q} V \xrightarrow{\tilde{B}} W
\]
\[
(u, v) \mapsto u \cdot v \mapsto B(u, v) = \tilde{B}(u \cdot v)
\]

(proof: compose with linear forms on \( W \) to reduce to the case \( W = \mathbb{F}_q \)).
**Lemma**

Let $\lambda_1, \ldots, \lambda_r$ be a basis of $V^\vee$. Then the $\frac{r(r+1)}{2}$ elements $\lambda_i \otimes^2$ for $1 \leq i \leq r$ and $(\lambda_i + \lambda_j) \otimes^2$ for $1 \leq i < j \leq r$ form a basis of $\text{Sym}(V; \mathbb{F}_q)$.

So we take \[ \left\{ \phi_1, \ldots, \phi_{\frac{r(r+1)}{2}} \right\} = \left\{ \lambda_i \right\}_{1 \leq i \leq r} \cup \left\{ \lambda_i + \lambda_j \right\}_{1 \leq i < j \leq r}. \]

Here $V = \mathbb{F}_{q^r}$. We get a unique $\theta$ with

\[
\begin{array}{rcl}
\mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \longrightarrow & \mathbb{F}_{q^r} \\
\phi \times \phi & \downarrow \quad & \uparrow \theta \\
\left( \mathbb{F}_q \right)^{\frac{r(r+1)}{2}} \times \left( \mathbb{F}_q \right)^{\frac{r(r+1)}{2}} & \longrightarrow & \left( \mathbb{F}_q \right)^{\frac{r(r+1)}{2}} \cong S_{\mathbb{F}_q}^2 \mathbb{F}_{q^r}
\end{array}
\]

and if we use $\phi$ to concatenate, the inner code has generating matrix

\[
G_\phi = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{pmatrix}.
\]
Does this help in understanding $\ker(\theta)$? Only a little bit...

Recall

\[
\mathbb{F}_{q^r} \otimes \mathbb{F}_{q^r} \xrightarrow{\sim} (\mathbb{F}_{q^r})^r \\
x \otimes y \mapsto (xy, xy^q, \ldots, xy^{q^{r-1}})
\]

so the composite map

\[
(\mathbb{F}_{q^r})^r \cong \mathbb{F}_{q^r} \otimes \mathbb{F}_{q^r} \longrightarrow S_{\mathbb{F}_q^2}^2 \mathbb{F}_{q^r} \xrightarrow{\theta} \mathbb{F}_{q^r}
\]

is projection on the first coordinate. But then???
Does this help in understanding $\ker(\theta)$? Only a little bit...

Recall

$$\mathbb{F}_{q^r} \otimes \mathbb{F}_{q^r} \xrightarrow{\sim} (\mathbb{F}_{q^r})^r$$

$$x \otimes y \mapsto (xy, xy^q, \ldots, xy^{q^{r-1}})$$

so the composite map

$$\left(\mathbb{F}_{q^r}\right)^r \simeq \mathbb{F}_{q^r} \otimes \mathbb{F}_{q^r} \longrightarrow S_{\mathbb{F}_q}^2 \mathbb{F}_{q^r} \xrightarrow{\theta} \mathbb{F}_{q^r}$$

is projection on the first coordinate. But then???
Does this help in understanding $\ker(\theta)$? Only a little bit...

Recall

$$\mathbb{F}_{q^r} \otimes \mathbb{F}_{q^r} \xrightarrow{\sim} (\mathbb{F}_{q^r})^r$$

$$x \otimes y \mapsto (xy, xy^q, \ldots, xy^{q^{r-1}})$$

so the composite map

$$((\mathbb{F}_{q^r})^r \simeq \mathbb{F}_{q^r} \otimes \mathbb{F}_{q^r} \longrightarrow S_{\mathbb{F}_q^2}^2 \mathbb{F}_{q^r} \longrightarrow \mathbb{F}_{q^r}$$

is projection on the first coordinate. But then???

(FAIL)

(well, not completely...)
Recall \( \text{Sym}(\mathbb{F}_{q^r}; \mathbb{F}_q) \) is generated by the \( \lambda \otimes^2 \) for \( \lambda \in \mathbb{F}_{q^r}^\times \). And each such \( \lambda \) is of the form \( \text{Tr}(a \cdot) \).

Now contemplate this formula:

\[
\text{Tr}(ax) \text{Tr}(ay) = (ax + a^q x^q + \cdots + a^{q^{r-1}} x^{q^{r-1}})(ay + a^q y^q + \cdots + a^{q^{r-1}} y^{q^{r-1}}) \\
= \text{Tr}(a^2 xy) + \sum_{1 \leq j \leq \lfloor r/2 \rfloor} \text{Tr}(a^{1+q^j} (xy^{q^j} + x^{q^j} y))
\]

(actually if \( r \) is even, the very last \( \text{Tr} \) should not be the trace from \( \mathbb{F}_{q^r} \) to \( \mathbb{F}_q \) but from \( \mathbb{F}_{q^{r/2}} \) to \( \mathbb{F}_q \)).
Recall $\text{Sym}(\mathbb{F}_q; \mathbb{F}_q)$ is generated by the $\lambda \otimes 2$ for $\lambda \in \mathbb{F}_{q^r}$. And each such $\lambda$ is of the form $\text{Tr}(a \cdot )$.

Now contemplate this formula:

$$\text{Tr}(ax) \text{Tr}(ay) = (ax + a^qx^q + \cdots + a^{q^{r-1}}x^{q^{r-1}})(ay + a^qy^q + \cdots + a^{q^{r-1}}y^{q^{r-1}})$$

$$= \text{Tr}(a^2xy) + \sum_{1 \leq j \leq \lfloor r/2 \rfloor} \text{Tr}(a^{1+q^j}(xy^{q^j} + x^{q^j}y))$$

(actually if $r$ is even, the very last $\text{Tr}$ should not be the trace from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ but from $\mathbb{F}_{q^{r/2}}$ to $\mathbb{F}_q$).

Let

$$m_0(x, y) = xy$$

and introduce higher twisted multiplication laws

$$m_j(x, y) = xy^{q^j} + x^{q^j}y$$

on $\mathbb{F}_{q^r}$ (actually if $r$ is even, $m_{r/2}$ takes values in $\mathbb{F}_{q^{r/2}}$).
The formula says that any symmetric bilinear form on $\mathbb{F}_{q^r}$ can be expressed in terms of traces and of the $m_j$. So in this way we can construct another basis of $\text{Sym}(\mathbb{F}_{q^r}; \mathbb{F}_q)$. Let’s sum all this up.
The formula says that any symmetric bilinear form on $\mathbb{F}_q^r$ can be expressed in terms of traces and of the $m_j$. So in this way we can construct another basis of $\text{Sym}(\mathbb{F}_q^r; \mathbb{F}_q)$. Let’s sum all this up.

Let

$$\Psi = (m_0, \ldots, m_{\lfloor r/2 \rfloor}) : \mathbb{F}_q^r \times \mathbb{F}_q^r \longrightarrow (\mathbb{F}_q^r)^{\frac{r+1}{2}}$$

(where by abuse of notation $(\mathbb{F}_q^r)^{\frac{r+1}{2}} = (\mathbb{F}_q^r)^{r/2} \times \mathbb{F}_q^{r/2}$ if $r$ is even).

Also recall

$$\Phi = (\phi_1 \otimes^2, \ldots, \phi_r \otimes^2) : \mathbb{F}_q^r \times \mathbb{F}_q^r \longrightarrow (\mathbb{F}_q)^{\frac{r(r+1)}{2}}.$$ 

Then $\Phi$ and $\Psi$ are two symmetric $\mathbb{F}_q$-bilinear maps that give two representations of $S^2_{\mathbb{F}_q} \mathbb{F}_q^r$ with its universal map $(x, y) \mapsto x \cdot y$ (and moreover $\Psi$ is a polynomial map over $\mathbb{F}_q^r$ of algebraic degree $1 + q^{\lfloor r/2 \rfloor}$).

By the universal property they are linked by some invertible $\mathbb{F}_q$-linear

$$\theta : (\mathbb{F}_q)^{\frac{r(r+1)}{2}} \sim (\mathbb{F}_q^r)^{\frac{r+1}{2}}.$$
Now we concatenate:

\[
C \times C \quad \xrightarrow{\Psi} \quad \langle \Psi(C, C') \rangle
\]

\[
\phi \times \phi \downarrow \quad \simeq \uparrow \theta
\]

\[
\phi(C') \times \phi(C') \quad \longrightarrow \quad \phi(C')^{\langle 2 \rangle}
\]

with

\[
\langle \Psi(C, C') \rangle \subset \langle m_0(C, C) \rangle \times \cdots \times \langle m_{\lfloor r/2 \rfloor}(C, C) \rangle
\]

and

\[
\langle m_j(C, C') \rangle \subset C^{\langle 1+q^j \rangle}.
\]
Now we concatenate:

\[
C \times C \xrightarrow{\Psi} \langle \Psi(C, C') \rangle
\]

\[
\phi \times \phi \downarrow \quad \cong \uparrow \theta
\]

\[
\phi(C) \times \phi(C') \longrightarrow \phi(C)^{(2)}
\]

with

\[
\langle \Psi(C, C') \rangle \subset \langle m_0(C, C) \rangle \times \cdots \times \langle m_{\lfloor r/2 \rfloor}(C, C) \rangle
\]

and

\[
\langle m_j(C, C') \rangle \subset C^{(1+q^j)}.
\]

Hence:

**Proposition**

\[
d_{\min}^{(2)}(\phi(C)) \geq d_{\min}^{(1+q^{\lfloor r/2 \rfloor})}(C)
\]
Let’s say $q = p$ is prime, for instance $q = 2$.

To conclude:
- $d_{\min}^{\langle 2 \rangle}(\phi(C)) \geq d_{\min}^{\langle 1+q^{\lceil r/2 \rceil} \rangle}(C)$
- take $C$ over $\mathbb{F}_{q^r}$ whose powers up to order $1 + q^{\lceil r/2 \rceil}$ are asymptotically good.

**Theorem 0:** possible up to order $\tau(q^r) \geq \lceil A(q^r) \rceil - 1$.

**Drinfeld-Vladut bound:** $A(q^r) \leq q^r/2 - 1$ with equality for $r$ even.

Of course we take $r$ even since we want $\tau(q^r)$ as big as possible.
Let’s say $q = p$ is prime, for instance $q = 2$.

To conclude:

- $d^{(2)}_{\min}(\phi(C)) \geq d^{(1+q^{[r/2]})}_{\min}(C)$
- take $C$ over $\mathbb{F}_{q^r}$ whose powers up to order $1 + q^{[r/2]}$ are asymptotically good.

**Theorem 0:** possible up to order $\tau(q^r) \geq \lceil A(q^r) \rceil - 1$.

Drinfeld-Vladut bound: $A(q^r) \leq q^r/2 - 1$ with equality for $r$ even.

Of course we take $r$ even since we want $\tau(q^r)$ as big as possible.

So we need powers up to order $1 + q^{r/2}$ and we have the estimate $q^{r/2} - 2$ for $\tau(q^r)$. 

Let’s say $q = p$ is prime, for instance $q = 2$.

To conclude:
- $d^{(2)}_{\min}(\phi(C)) \geq d^{(1+q^{[r/2]})}_{\min}(C)$
- take $C$ over $\mathbb{F}_{q^r}$ whose powers up to order $1 + q^{[r/2]}$ are asymptotically good.

Theorem 0: possible up to order $\tau(q^r) \geq \lceil A(q^r) \rceil - 1$.

Drinfeld-Vladut bound: $A(q^r) \leq q^r/2 - 1$ with equality for $r$ even.

Of course we take $r$ even since we want $\tau(q^r)$ as big as possible.
So we need powers up to order $1 + q^{r/2}$ and we have the estimate $q^{r/2} - 2$ for $\tau(q^r)$.... Not enough!
Why not try something stupid? Take $r$ odd.

Then $1 + q^{[r/2]} < \lceil q^{r/2} - 1 \rceil - 1$ so there is some (little) room below Drinfeld-Vladut. But does $A(q^r)$ fit in between?

Yes: for $q$ prime, a recent construction of Garcia-Stichtenoth-Bassa-Beelen gives

$$A(q^r) \geq \left( \frac{2q}{q + 1} + o(1) \right) q^{[r/2]}$$

when $r \to \infty$ odd.
Why not try something stupid? Take $r$ odd.
Then $1 + q^{\lfloor r/2 \rfloor} < \lceil q^{r/2} - 1 \rceil - 1$ so there is some (little) room below Drinfeld-Vladut. But does $A(q^r)$ fit in between?
Yes: for $q$ prime, a recent construction of Garcia-Stichtenoth-Bassa-Beelen gives
\[
A(q^r) \geq (\frac{2q}{q+1} + o(1))q^{\lfloor r/2 \rfloor}
\]
when $r \to \infty$ odd.
Actually for $q = 2$ we take $r = 9$. GSBB gives $A(512) \geq 465/23 \approx 20.217$.

Theorem 0: $\alpha^{\langle 17 \rangle}_{512}(\delta) \geq \frac{1-\delta}{17} - \frac{1}{A(512)}$.

The concatenation map $\phi$ has parameters $[45, 9]$ hence
\[
\alpha^{\langle 2 \rangle}_{2}(\delta) \geq \frac{1}{5} \alpha^{\langle 17 \rangle}_{512}(45\delta)
\]
which is Theorem 1.