Asymptotically good binary linear codes with asymptotically good self-intersection spans

Hugues Randriambololona

August 31, 2012

Abstract

If C is a binary linear code, let $C^{\langle 2\rangle}$ be the linear code spanned by intersections of pairs of codewords of C. We construct an asymptotically good family of binary linear codes such that, for C ranging in this family, the $C^{\langle 2\rangle}$ also form an asymptotically good family. For this we use algebraic-geometry codes, concatenation, and a fair amount of bilinear algebra.

More precisely, the two main ingredients used in our construction are, first, a description of the symmetric square of an odd degree extension field in terms only of field operations of small degree, and second, a recent result of Garcia-Stichtenoth-Bassa-Beelen on the number of points of curves on such an odd degree extension field.

1 Statement of result

Let q be a prime power, and $\mathbb{F}_q$ the field with q elements. For any integer $n \geq 1$, let $*$ denote coordinatewise multiplication in the vector space $(\mathbb{F}_q)^n$, so

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

For $C \subset (\mathbb{F}_q)^n$ a linear subspace, *i.e.* a q-ary linear code of length n, let

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

and let

$$C^{\langle 2\rangle} = \langle C * C\rangle = \{ \sum_{c,c' \in C} \alpha_{c,c'} c * c' \mid \alpha_{c,c'} \in \mathbb{F}_q\} \tag{1}$$

be the *linear span* of $C * C$. In fact the set $C * C$ is stable under multiplication by scalars (because C is), so $C^{\langle 2\rangle}$ can equivalently be defined as just the *additive span* of $C * C$.

Remark that the support of $c * c'$ is the intersection of the supports of c and c'. We then call $C^{\langle 2\rangle}$ the *self-intersection span* of C. We will be especially interested in the case $q = 2$, where a codeword can indeed be identified with its support, unambiguously. Sometimes we will also call $C^{\langle 2\rangle}$ the “square” of C, and more generally, higher "powers" $C^{\langle t\rangle}$ can be defined analogously, for any $t \geq 0$ (see section 4).

Write $\mathrm{R}(C)$ and $\delta(C)$ for the rate and relative minimum distance of C. As a shortcut, write also $\mathrm{R}^{\langle 2\rangle}(C) = \mathrm{R}(C^{\langle 2\rangle})$ and $\delta^{\langle 2\rangle}(C) = \delta(C^{\langle 2\rangle})$. It is easily seen that these functions satisfy:

$$\mathrm{R}^{\langle 2\rangle} \geq \mathrm{R} \qquad\qquad \delta^{\langle 2\rangle} \leq \delta \tag{2}$$

(see Proposition 11 below; for $q = 2$ one even has the stronger result that C is a subcode of $C^{\langle 2\rangle}$, since then $c * c = c$ for all c).

Recall that a family of codes C_i of length going to infinity is said *asymptotically good* if both $\mathrm{R}(C_i)$ and $\delta(C_i)$ admit a positive asymptotic lower bound.

Theorem 1. *For any prime power q (*e.g. $q = 2$*), there exists an asymptotically good family of q-ary linear codes C_i whose self-intersection spans $C_i^{\langle 2\rangle}$ also form an asymptotically good family.*

Keeping (2) in mind, we can rephrase the theorem as asking for $\varepsilon, \varepsilon' > 0$ such that $\liminf_i \mathrm{R}(C_i) \geq \varepsilon$ and $\liminf_i \delta^{\langle 2\rangle}(C_i) \geq \varepsilon'$. Our proof will be constructive, for example for $q = 2$ we will give an explicit construction with $\varepsilon = 1/651$ and $\varepsilon' = 1/1575$ (more generally all the parameter domain $\varepsilon \leq 0.001872 - 0.5294\,\varepsilon'$ can be attained).

Apparently the question of the existence of such codes was first raised by G. Zémor. The author's interest in it started from a suggestion of C. Xing. The generalization to cubes of codes, or to arbitrarily high powers, is still open (of course the case of real interest is $q = 2$).

While study of the behavior of linear codes under the operation $*$ is a very natural problem and certainly deserves investigation for its own sake, motivation comes as well from applications, such as the analysis of bilinear algorithms [9]. There are also links with secret-sharing and multi-party computation systems [2][3]. More precisely, suppose given a symmetric $\mathbb{F}_q$-bilinear map $B : V \times V \longrightarrow W$, where V, W are finite dimensional $\mathbb{F}_q$-vector spaces, as well as a pair of $\mathbb{F}_q$-linear maps $\phi : V \longrightarrow (\mathbb{F}_q)^n$ and $\theta : (\mathbb{F}_q)^n \longrightarrow W$, such that the following diagram commutes:

$$\begin{array}{ccc} V \times V & \xrightarrow{B} & W \\ {\scriptstyle \phi\times\phi}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array} \tag{3}$$

that is, such that $B(u, v) = \theta(\phi(u) * \phi(v))$ for all $u, v \in V$.

From the point of view of algebraic complexity theory, diagram (3) expresses how to compute B using only n two-variable multiplications in $\mathbb{F}_q$. The two maps ϕ, θ are then said to define a *(symmetric) bilinear algorithm* of length n for B. Of particular interest is the case where $V = W = \mathbb{F}_{q^r}$ is an extension field of $\mathbb{F}_q$ and B is usual field multiplication in it: we refer the reader to [1][4][11] for recent results on this topic. On the other hand, from the point of view of secret-sharing and multi-party computation, diagram (3) can be interpreted as follows: elements $u, v \in V$ are split into shares according to ϕ and distributed to n remote users, these users then multiply their shares locally, and finally their local results are combined with θ to get $B(u, v)$. Several refinements can then be considered.

First, remark that given finitely many $u^{(i)}, v^{(i)} \in V$, a more general expression such as

$$\begin{aligned}\sum_i B(u^{(i)}, v^{(i)}) &= \sum_i \theta(\phi(u^{(i)}) * \phi(v^{(i)})) \\ &= \theta(\sum_i \phi(u^{(i)}) * \phi(v^{(i)}))\end{aligned}$$

can be computed by applying θ only once, at the very end. Moreover, letting $C \subset (\mathbb{F}_q)^n$ be the image of ϕ, we see that the sum $s = \sum_i \phi(u^{(i)}) * \phi(v^{(i)})$ to which θ is applied at the end of the computation, describes a generic element of $C^{\langle 2 \rangle}$. Depending on the context, it could then be desirable that this computation be resistant to local alterations of s caused by noise, or by unreliable users. Also, in a scenario à la threshold cryptography, an important feature will be the ability to reconstruct $B(u, v)$ knowing only a certain given number of coordinates of s. Clearly, all these properties will be controlled by the minimum distance of $C^{\langle 2 \rangle}$.

2 Some ideas behind the proof

Here we discuss informally some ideas that lead to the proof of Theorem 1. Certainly this discussion reflects only the author's own experience in dealing with this problem. Since it is not logically necessary for the understanding of the proof, the reader can skip it with no harm and go directly to the next section (and maybe come back here later).

There is a certain similarity between our object of interest and the theory of linear intersecting codes [5][10]. Recall that a linear code C is said intersecting if $c * c'$ is non-zero for all non-zero $c, c' \in C$ (and this could be refined by requiring $c * c'$ to have at least a certain prescribed weight). Although none of these notions imply the other, it turns out that methods used to produce intersecting codes often produce codes having a good $\delta^{\langle 2 \rangle}$. This is often the case, for example, for intersecting codes constructed as evaluation codes (see [12][13] for more on this topic, although actually the codes constructed there do not have a good $\delta^{\langle 2 \rangle}$).

Suppose we are given an algebra $\mathcal{F}$ of functions, admitting a nice notion of "degree", and which can be evaluated at a certain set of points X. We then define a linear code C_D as the image of the space $\mathcal{F}(D)$ of functions of degree at most D under this evaluation map. For example, $\mathcal{F}$ could be the algebra of polynomials in one or several indeterminates over a finite field, giving rise to Reed-Solomon or Reed-Muller codes. Or $\mathcal{F}$ could be the function field of an algebraic curve, giving rise to Goppa's algebraic-geometry codes. In all these situations, bounds on the parameters of C_D can be deduced from D and the cardinality of X. Now for $f, f' \in \mathcal{F}(D)$ we have $ff' \in \mathcal{F}(2D)$, which implies $c * c' \in C_{2D}$ for all $c, c' \in C_D$. Applying the aforementioned bounds to C_{2D}, we find that C_D is intersecting provided D is suitably chosen. But in fact, by linearity, the argument just above gives the stronger result $C_D^{\langle 2\rangle} \subset C_{2D}$, from which the lower bound $\delta^{\langle 2\rangle}(C_D) \geq \delta(C_{2D})$ follows.

Remark then that to have a lower bound on $\mathrm{R}(C_D)$ requires in general D to be large, while a lower bound on $\delta(C_{2D})$ requires $2D$ to be small with respect to the cardinality of X. When the size q of the field is big enough, these two conditions are compatible: for example, algebraic-geometry codes verifying the hypotheses in Theorem 1 can be constructed as soon as the Ihara constant satisfies $A(q) > 2$ (see sections 5 and 6). Unfortunately, with the present techniques, if q is too small, these two requirements become contradictory when one lets the length of the codes go to infinity. A standard solution in such a situation is to work first over an extension field, and then conclude with a concatenation argument. If one is interested only in constructing intersecting codes, this works easily [12] because a concatenation of intersecting codes is intersecting. But in the problem we study, things do not behave so nicely: in general it appears very difficult to derive a lower bound on the $\delta^{\langle 2\rangle}$ of a concatenated code from the parameters of its inner and outer codes. Perhaps this is best illustrated as follows.

Let $\mathbb{F}_{q^r}$ be an extension of $\mathbb{F}_q$, and let $\phi : \mathbb{F}_{q^r} \longrightarrow (\mathbb{F}_q)^l$ and $\theta : (\mathbb{F}_q)^l \longrightarrow \mathbb{F}_{q^r}$ define a multiplication algorithm as discussed in the previous section, so $xy = \theta(\phi(x) * \phi(y))$ for all $x, y \in \mathbb{F}_{q^r}$. A very tempting approach when trying to prove Theorem 1 is then to concatenate codes C having asymptotically good squares over an extension field $\mathbb{F}_{q^r}$, with ϕ. For if $\phi(C)$ denotes the concatenated code, it is easily seen that θ maps $\phi(C)^{\langle 2\rangle}$ in $C^{\langle 2\rangle}$, hence one could hope to use this "reconstruction map" to derive a lower bound on the minimum distance of $\phi(C)^{\langle 2\rangle}$ from that of $C^{\langle 2\rangle}$. More precisely, if $c \in \phi(C)^{\langle 2\rangle}$ has weight less than $d = \mathrm{d}_{\min}(C^{\langle 2\rangle})$, then a fortiori c has less than d non-zero block symbols over $(\mathbb{F}_q)^l$, so $\theta(c) \in C^{\langle 2\rangle}$ has weight less than d, hence $\theta(c) = 0$. If θ were injective, we could deduce that $c = 0$. Unfortunately, for $r > 1$ it turns out that θ is never injective, and all we get is that the block symbols of c all live in $\ker(\theta)$. So this "naive approach" fails, but not by much: the obstruction is the kernel of θ.

We fix this as follows. In section 3 we define higher "twisted multiplication laws" m_j on $\mathbb{F}_{q^r}$, and we put them together in a map $\Psi : \mathbb{F}_{q^r} \times \mathbb{F}_{q^r} \longrightarrow W$, where $W = (\mathbb{F}_{q^r})^{\lceil \frac{r}{2} \rceil}$ if r is odd (and $W = (\mathbb{F}_{q^r})^{\frac{r}{2}} \times \mathbb{F}_{q^{\frac{r}{2}}}$ if r is even), so that:

- over $\mathbb{F}_q$, Ψ is symmetric bilinear
- over $\mathbb{F}_{q^r}$, Ψ is a polynomial map of degree $1 + q^{\lfloor \frac{r}{2} \rfloor}$.

We then construct a bilinear algorithm

$$\begin{array}{ccc} \mathbb{F}_{q^r} \times \mathbb{F}_{q^r} & \xrightarrow{\Psi} & W \\ {\scriptstyle \phi\times\phi}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^{\frac{r(r+1)}{2}} \times (\mathbb{F}_q)^{\frac{r(r+1)}{2}} & \xrightarrow{*} & (\mathbb{F}_q)^{\frac{r(r+1)}{2}} \end{array} \qquad (4)$$

with the property that θ is *bijective*. The key steps in proving the bijectivity of θ are:

- identify the lower right $(\mathbb{F}_q)^{\frac{r(r+1)}{2}}$ in (4) with the symmetric square $S^2_{\mathbb{F}_q}\mathbb{F}_{q^r}$, that is, with the space through which any symmetric $\mathbb{F}_q$-bilinear map on $\mathbb{F}_{q^r}$ factorizes uniquely
- remark that any symmetric $\mathbb{F}_q$-bilinear map on $\mathbb{F}_{q^r}$ can be expressed uniquely in terms of the m_j for $0 \leq j \leq \lfloor \frac{r}{2} \rfloor$, and $\mathbb{F}_q$-linear operations.

We can then concatenate with ϕ as in the naive approach above. In appropriate bases, the matrix of ϕ, that is, the generating matrix of the inner code, is made of all $\{0,1\}$ columns of weight 1 or 2. For example, for $r = 4$, it would look like

$$G_\phi = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

although actually (for $q = 2$) we will take $r = 9$.

Now θ has no kernel, so we can derive a lower bound on the minimum distance of the squared concatenated code $\phi(C)^{\langle 2 \rangle}$ by the very same argument as sketched above. This is done in section 4. However there is then an added difficulty: since Ψ has degree $1 + q^{\lfloor \frac{r}{2} \rfloor}$, this bound will not be in terms of the minimum distance of the square of the outer code C only, but also that of its higher powers up to order $1 + q^{\lfloor \frac{r}{2} \rfloor}$.

So to conclude (sections 5 and 6) we need codes over $\mathbb{F}_{q^r}$ whose powers up to order $1 + q^{\lfloor \frac{r}{2} \rfloor}$ are asymptotically good. On the other hand, algebraic geometry provides codes over $\mathbb{F}_{q^r}$ whose powers up to order $\lceil A(q^r) \rceil - 1$ are asymptotically good. When r is even, this is not enough: because there we have $\lfloor \frac{r}{2} \rfloor = \frac{r}{2}$ and we face the Drinfeld-Vladut bound [6] $A(q^r) \leq q^{\frac{r}{2}} - 1$. However, when r is odd, we have $\lfloor \frac{r}{2} \rfloor = \frac{r-1}{2}$, which leaves us just enough room under the Drinfeld-Vladut bound to make use of a recent construction [7] of Garcia-Stichtenoth-Bassa-Beelen, that provides us with curves sufficiently close to it (although not attaining it) to meet our needs.

3 Bilinear study of field extensions

Let V be a vector space of dimension r over $\mathbb{F}_q$, and let $V^\vee$ be its dual vector space. Let also $\mathrm{Sym}(V;\mathbb{F}_q)$ be the space of symmetric bilinear forms on V. If $\lambda \in V^\vee$ is a linear form on V, we can define

$$\begin{array}{rccc} \lambda^{\otimes 2}: & V \times V & \longrightarrow & \mathbb{F}_q \\ & (u,v) & \mapsto & \lambda(u)\lambda(v) \end{array}$$

which is a symmetric bilinear form on V.

Lemma 2. *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* $\mathrm{Sym}(V; \mathbb{F}_q)$.

Proof. Using $\lambda_1, \ldots, \lambda_r$ as coordinate functions we can suppose $V = (\mathbb{F}_q)^r$. Then $\lambda_i^{\otimes 2}$ is the symmetric bilinear form

$$(u, v) \mapsto u_i v_i \tag{5}$$

and $(\lambda_i + \lambda_j)^{\otimes 2}$ is $(u, v) \mapsto (u_i + u_j)(v_i + v_j)$, hence $(\lambda_i + \lambda_j)^{\otimes 2} - \lambda_i^{\otimes 2} - \lambda_j^{\otimes 2}$ is

$$(u, v) \mapsto u_i v_j + u_j v_i. \tag{6}$$

Then we conclude by recognizing these (5) and (6) as forming the standard basis of $\mathrm{Sym}((\mathbb{F}_q)^r; \mathbb{F}_q)$. $\square$

We will now be interested in the case $V = \mathbb{F}_{q^r}$ is an extension field, which can indeed be considered as a vector space over $\mathbb{F}_q$, and we let $\gamma_1, \ldots, \gamma_r$ be a basis (for example $\gamma_i = \gamma^{i-1}$ for some choice of a primitive element $\gamma \in \mathbb{F}_{q^r}$). Let also $\mathrm{Tr} : \mathbb{F}_{q^r} \longrightarrow \mathbb{F}_q$ denote the trace function. To each $a \in \mathbb{F}_{q^r}$ we can associate a linear form

$$\begin{array}{rccc} t_a : & \mathbb{F}_{q^r} & \longrightarrow & \mathbb{F}_q \\ & x & \mapsto & \mathrm{Tr}(ax). \end{array}$$

The following is well known:

Lemma 3. *The map*

$$\begin{array}{ccc} \mathbb{F}_{q^r} & \longrightarrow & (\mathbb{F}_{q^r})^\vee \\ a & \mapsto & t_a \end{array}$$

is an isomorphism of $\mathbb{F}_q$-vector spaces. In particular, $t_{\gamma_1}, \ldots, t_{\gamma_r}$ form a basis of $(\mathbb{F}_{q^r})^\vee$.

As a field, $\mathbb{F}_{q^r}$ is endowed with its usual multiplication law, which we will denote by m_0, so

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

for $x, y \in \mathbb{F}_{q^r}$. For any integer $j \geq 1$, we can also define a "twisted multiplication law" m_j by

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

Remark that these maps are symmetric and $\mathbb{F}_q$-bilinear (although not $\mathbb{F}_{q^r}$-bilinear in general).

Proposition 4. *Choose an ordering of the set $\{t_{\gamma_i}\}_{1 \leq i \leq r} \cup \{t_{\gamma_i + \gamma_j}\}_{1 \leq i < j \leq r}$ and rename its elements accordingly, say:*

$$\{t_{\gamma_i}\}_{1 \leq i \leq r} \cup \{t_{\gamma_i + \gamma_j}\}_{1 \leq i < j \leq r} = \{\phi_1, \ldots, \phi_{\frac{r(r+1)}{2}}\}.$$

Then:

- *The family*
$$(\phi_1^{\otimes 2}, \ldots, \phi_{\frac{r(r+1)}{2}}^{\otimes 2})$$
is a basis of $\mathrm{Sym}(\mathbb{F}_{q^r}; \mathbb{F}_q)$.

- *If* $r = 2s+1$ *is odd, the family*
$$(t_{\gamma_i} \circ m_j)_{\substack{1 \le i \le r \\ 0 \le j \le s}}$$
is a basis of $\mathrm{Sym}(\mathbb{F}_{q^r}; \mathbb{F}_q)$.

Proof. The first claim is a consequence of Lemma 2 and Lemma 3. To prove the second claim, start by remarking that the given family has the correct size $r(s+1) = \frac{r(r+1)}{2}$. It suffices thus to show that it is a generating family, and for this (because of the first claim) it suffices to show that each $t_a^{\otimes 2}$, for $a \in \mathbb{F}_{q^r}$, can be written as a linear combination of the $t_b \circ m_j$, for $b \in \mathbb{F}_{q^r}$ and $0 \le j \le s$. However for any $x, y \in \mathbb{F}_{q^r}$ we have

$$\begin{aligned} \mathrm{Tr}(ax)\,\mathrm{Tr}(ay) &= (ax + a^q x^q + \cdots + a^{q^{2s}} x^{q^{2s}})(ay + a^q y^q + \cdots + a^{q^{2s}} y^{q^{2s}}) \\ &= \mathrm{Tr}(a^2 xy) + \sum_{1 \le j \le s} \mathrm{Tr}(a^{1+q^j}(xy^{q^j} + x^{q^j} y)) \end{aligned}$$

which can be restated
$$t_a^{\otimes 2} = \sum_{0 \le j \le s} t_{a^{1+q^j}} \circ m_j$$
as wanted. □

From now on we suppose $r = 2s+1$ is odd, so $\frac{r(r+1)}{2} = (s+1)(2s+1)$. Consider the symmetric $\mathbb{F}_q$-bilinear maps

$$\Phi = (\phi_1^{\otimes 2}, \ldots, \phi_{(s+1)(2s+1)}^{\otimes 2}) : \mathbb{F}_{q^{2s+1}} \times \mathbb{F}_{q^{2s+1}} \longrightarrow (\mathbb{F}_q)^{(s+1)(2s+1)}$$

and
$$\Psi = (m_0, \ldots, m_s) : \mathbb{F}_{q^{2s+1}} \times \mathbb{F}_{q^{2s+1}} \longrightarrow (\mathbb{F}_{q^{2s+1}})^{s+1}.$$

Proposition 4 can then be restated as follows:

Corollary 5. *There is an isomorphism of* $\mathbb{F}_q$*-vector spaces*
$$\theta : (\mathbb{F}_q)^{(s+1)(2s+1)} \xrightarrow{\sim} (\mathbb{F}_{q^{2s+1}})^{s+1}$$
such that
$$\theta \circ \Phi = \Psi.$$

Proof. Set $r = 2s+1$, use the t_{γ_i} as coordinate functions on $\mathbb{F}_{q^r}$ as allowed by Lemma 3, and define θ as the invertible linear transformation that maps the first basis of $\mathrm{Sym}(\mathbb{F}_{q^r}; \mathbb{F}_q)$ given in Proposition 4 to the second one. □

Remark 6. For the more sophisticated reader, recall that the symmetric square of a vector space V over $\mathbb{F}_q$ can be defined, for our purpose, as the dual of the space of symmetric bilinear forms on it: $S^2_{\mathbb{F}_q}V = \mathrm{Sym}(V;\mathbb{F}_q)^\vee$. We let $(u,v) \mapsto u \cdot v$ be the universal symmetric bilinear map $V \times V \longrightarrow S^2_{\mathbb{F}_q}V$, where $u \cdot v \in S^2_{\mathbb{F}_q}V$ is the "evaluation" element that sends $F \in \mathrm{Sym}(V;\mathbb{F}_q)$ to $F(u,v)$. Recall also the universal property of the symmetric square: for any $\mathbb{F}_q$-vector space W, there is a natural identification

$$\left\{ \begin{array}{c} \text{symmetric bilinear maps} \\ V \times V \longrightarrow W \end{array} \right\} = \left\{ \begin{array}{c} \text{linear maps} \\ S^2_{\mathbb{F}_q}V \longrightarrow W \end{array} \right\}$$

as $\mathbb{F}_q$-vector spaces, where a linear map $f : S^2_{\mathbb{F}_q}V \longrightarrow W$ corresponds to the symmetric bilinear map $(u,v) \mapsto f(u \cdot v)$.

So, in the case $V = \mathbb{F}_{q^{2s+1}}$, the symmetric bilinear maps Φ and Ψ give rise to linear maps $\overline{\Phi}$ and $\overline{\Psi}$ on $S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s+1}}$, and Proposition 4 expresses that these

$$\begin{array}{rccc} \overline{\Phi}: & S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s+1}} & \xrightarrow{\sim} & (\mathbb{F}_q)^{(s+1)(2s+1)} \\ & x \cdot y & \mapsto & (\phi_1(x)\phi_1(y),\, \phi_2(x)\phi_2(y),\, \dots) \end{array}$$

and

$$\begin{array}{rccc} \overline{\Psi}: & S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s+1}} & \xrightarrow{\sim} & (\mathbb{F}_{q^{2s+1}})^{s+1} \\ & x \cdot y & \mapsto & (xy,\, xy^q + x^q y,\, \dots,\, xy^{q^s} + x^{q^s}y) \end{array}$$

are isomorphisms of $\mathbb{F}_q$-vector spaces (while $\theta = \overline{\Psi} \circ \overline{\Phi}^{-1}$ in Corollary 5).

A similar result can be given in the case of an even degree extension $\mathbb{F}_{q^{2s}}$, with only one minor change. Indeed, in this case remark that one has $(xy^{q^s} + x^{q^s}y)^{q^s} = x^{q^s}y + xy^{q^s}$ for all $x, y \in \mathbb{F}_{q^{2s}}$, which means that m_s takes values in the subfield $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^{2s}}$. Then the very same arguments as before show that $m_0, \dots, m_s$ induce an isomorphism of $\mathbb{F}_q$-vector spaces

$$S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s}} \xrightarrow{\sim} (\mathbb{F}_{q^{2s}})^s \times \mathbb{F}_{q^s},$$

and composing with traces gives a basis of $\mathrm{Sym}(\mathbb{F}_{q^{2s}};\mathbb{F}_q)$ in this case also.

4 Bilinear study of concatenated codes

If $\mathcal{A}$ is a vector space of finite dimension over $\mathbb{F}_q$, if $n \geq 1$ is an integer and $C \subset \mathcal{A}^n$ is a linear subspace, and if $f : \mathcal{A} \longrightarrow \mathcal{B}$ is a linear map from $\mathcal{A}$ to another vector space $\mathcal{B}$, we denote by $f(C) \subset \mathcal{B}^n$ the subspace obtained by applying f componentwise to the "codewords" of C:

$$f(C) = \{(f(c_1), \dots, f(c_n)) \in \mathcal{B}^n \mid c = (c_1, \dots, c_n) \in C \subset \mathcal{A}^n\}.$$

Also if $C' \subset \mathcal{A}'^n$ is a code of the same length over another linear alphabet $\mathcal{A}'$, and if $F : \mathcal{A} \times \mathcal{A}' \longrightarrow \mathcal{B}$ is a bilinear map, we denote by $\langle F(C, C') \rangle \subset \mathcal{B}^n$ the linear span of the set of elements obtained by applying F componentwise to pairs of codewords in C and C':

$$\langle F(C,C')\rangle = \{\textstyle\sum_{\substack{c\in C\\ c'\in C'}} \alpha_{c,c'}(F(c_1,c'_1),\dots,F(c_n,c'_n)) \mid \alpha_{c,c'}\in\mathbb{F}_q\} \tag{7}$$

which generalizes (1).

We will be interested in the case $\mathcal{A}=\mathbb{F}_{q^{2s+1}}$ is an odd degree extension field of $\mathbb{F}_q$. Recall the notations from the previous section. First we have the linear map

$$\phi=(\phi_1,\dots,\phi_{(s+1)(2s+1)}):\mathbb{F}_{q^{2s+1}}\longrightarrow(\mathbb{F}_q)^{(s+1)(2s+1)}$$

as well as the symmetric bilinear map

$$\Phi=(\phi_1^{\otimes 2},\dots,\phi_{(s+1)(2s+1)}^{\otimes 2}):\mathbb{F}_{q^{2s+1}}\times\mathbb{F}_{q^{2s+1}}\longrightarrow(\mathbb{F}_q)^{(s+1)(2s+1)}.$$

If $C\subset(\mathbb{F}_{q^{2s+1}})^n$ is a linear code of length n over $\mathbb{F}_{q^{2s+1}}$, we will consider $\phi(C)$ and $\langle\Phi(C,C)\rangle$ as codes of length $N=(s+1)(2s+1)n$ over $\mathbb{F}_q$, using the natural identification $((\mathbb{F}_q)^{(s+1)(2s+1)})^n=(\mathbb{F}_q)^N$. Then:

Lemma 7. *With these notations,*

$$\langle\Phi(C,C)\rangle=\phi(C)^{\langle 2\rangle}.$$

Proof. Direct consequence of the definitions. □

We also have the symmetric $\mathbb{F}_q$-bilinear maps

$$m_j:\mathbb{F}_{q^{2s+1}}\times\mathbb{F}_{q^{2s+1}}\longrightarrow\mathbb{F}_{q^{2s+1}}$$

for $0\le j\le s$, from which we formed

$$\Psi=(m_0,\dots,m_s):\mathbb{F}_{q^{2s+1}}\times\mathbb{F}_{q^{2s+1}}\longrightarrow(\mathbb{F}_{q^{2s+1}})^{s+1}.$$

Remark that m_0 is not only $\mathbb{F}_q$-bilinear, it is also $\mathbb{F}_{q^{2s+1}}$-bilinear. So if the code $C\subset(\mathbb{F}_{q^{2s+1}})^n$ is $\mathbb{F}_{q^{2s+1}}$-linear, then so is $\langle m_0(C,C)\rangle$. In fact $\langle m_0(C,C)\rangle=C^{\langle 2\rangle}$ provided now componentwise multiplication $*$ is meant over $\mathbb{F}_{q^{2s+1}}$.

On the other hand, for $j\ge 1$, m_j is only $\mathbb{F}_q$-bilinear. So $\langle m_j(C,C)\rangle$ will only be a $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_{q^{2s+1}})^n$ (and similarly for $\langle\Psi(C,C)\rangle$). Nevertheless we will still define the weight of a codeword in $\langle m_j(C,C)\rangle$ and the minimum distance $\mathrm{d_{min}}(\langle m_j(C,C)\rangle)$ as the usual weight and distance taken in $(\mathbb{F}_{q^{2s+1}})^n$, that is, over the alphabet $\mathbb{F}_{q^{2s+1}}$.

Proposition 8. *With the notations above,*

$$\mathrm{d_{min}}(\phi(C)^{\langle 2\rangle})\ge\min_{0\le j\le s}\mathrm{d_{min}}(\langle m_j(C,C)\rangle).$$

Proof. Let $c \in \phi(C)^{\langle 2\rangle}$ be a codeword. We have to show that if c has weight

$$w < \mathrm{d}_{\min}(\langle m_j(C,C)\rangle) \tag{8}$$

for all $0 \leq j \leq s$, then it is the zero codeword.

Here c is seen as a word of length N over the alphabet $\mathbb{F}_q$, but we can also see it as a word of length n over the alphabet $(\mathbb{F}_q)^{(s+1)(2s+1)}$, and as such obviously it has weight

$$\widetilde{w} \leq w. \tag{9}$$

Now, using Corollary 5 and Lemma 7, we apply θ blockwise to get a codeword $\theta(c) \in \langle\Psi(C,C)\rangle$. Since θ is invertible, we see that, considered as a word of length n over the alphabet $(\mathbb{F}_{q^{2s+1}})^{s+1}$, this $\theta(c)$ has the same weight $\widetilde{w}$.

If we denote by $\pi_0,\dots,\pi_s$ the $s+1$ coordinate projections $(\mathbb{F}_{q^{2s+1}})^{s+1} \longrightarrow \mathbb{F}_{q^{2s+1}}$, then by construction we have $m_j = \pi_j \circ \Psi$, so applying π_j blockwise we get a codeword $\pi_j(\theta(c)) \in \langle m_j(C,C)\rangle$, of weight at most $\widetilde{w}$. But then, $\pi_j(\theta(c))$ is the zero codeword because of (8) and (9), and since this holds for all j, we conclude that $\theta(c)$ is zero, hence c is zero. $\square$

Remark 9. This is a continuation of Remark 6. Recall from the symmetric square construction that we have a universal product $\cdot : \mathbb{F}_{q^{2s+1}} \times \mathbb{F}_{q^{2s+1}} \longrightarrow S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s+1}}$. The underlying notion in the proof of Proposition 8 is then that of the "universal symmetric bilinear span"

$$\langle C \cdot C\rangle \subset (S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s+1}})^n$$

constructed from C and $\cdot$ as in (7), and of which $\langle\Phi(C,C)\rangle = \phi(C)^{\langle 2\rangle}$ and $\langle\Psi(C,C)\rangle$ are two incarnations, under the invertible linear changes of alphabets $\overline{\Phi}$ and $\overline{\Psi}$. In particular the weight $\widetilde{w}$ in (9) should be interpreted as the weight of c considered as a word over the alphabet $S^2_{\mathbb{F}_q}\mathbb{F}_{q^{2s+1}}$.

Now let K be a finite field (we will apply both cases $K = \mathbb{F}_q$ and $K = \mathbb{F}_{q^{2s+1}}$), and let $*$ denote coordinatewise multiplication in the vector space K^n, which is a symmetric K-bilinear map $K^n \times K^n \longrightarrow K^n$. If $C, C' \subset K^n$ are two linear codes of the same length, we can define their intersection span

$$\langle C * C'\rangle \subset K^n$$

as in (7), and iteratively, setting $C^{<0>}$ as the $[n,1,n]$ repetition code, we can define *higher self-intersection spans* (or "powers")

$$C^{\langle t+1\rangle} = \langle C^{\langle t\rangle} * C\rangle$$

for $t \geq 0$. Equivalently, $C^{\langle t\rangle}$ is the linear span of the set of coordinatewise products of t-uples of codewords from C.

In particular we have $C^{\langle 1\rangle} = C$, and $C^{\langle 2\rangle}$ is the same as in (1). More generally we have the natural identities

$$\langle C^{\langle t\rangle} * C^{\langle t'\rangle}\rangle = C^{\langle t+t'\rangle}$$

and

$$(C^{\langle t\rangle})^{\langle t'\rangle} = C^{\langle tt'\rangle}.$$

Lemma 10. *Let $t \geq 1$. If $c \in C^{\langle t\rangle}$ is a codeword and if i is a coordinate at which c is non-zero, then there is already some $c' \in C$ that is non-zero at i.*

Proof. Obvious. $\square$

Now given a linear code $C \subset K^n$, for each integer $t \geq 0$, we can define the "higher" dimension $\dim^{\langle t\rangle}$, distance $\mathrm{d}_{\min}^{\langle t\rangle}$, rate $\mathrm{R}^{\langle t\rangle}$, and relative distance $\delta^{\langle t\rangle}$ of C, as those parameters for $C^{\langle t\rangle}$. Then:

Proposition 11. *Let C be a (non-zero) linear code. Then for all $t \geq 0$, we have*

$$\dim^{\langle t+1\rangle}(C) \geq \dim^{\langle t\rangle}(C)$$

and

$$\mathrm{d}_{\min}^{\langle t+1\rangle}(C) \leq \mathrm{d}_{\min}^{\langle t\rangle}(C).$$

Proof. For $t = 0$ these inequalities hold by convention, so we suppose $t \geq 1$. Let $k_t = \dim^{\langle t\rangle}(C)$, and let $S \subset \{1, \ldots, n\}$ be an information set of coordinates for $C^{\langle t\rangle}$. Without loss of generality we can suppose $S = \{1, \ldots, k_t\}$. Let G_t be the generating matrix of $C^{\langle t\rangle}$ put in systematic form with respect to S. If c is the i-th line of G_t, then $c \in C^{\langle t\rangle}$ has a 1 at coordinate i and is zero over $S \setminus \{i\}$. By Lemma 10 we can find $c' \in C$ that is non-zero at i, hence $c * c' \in C^{\langle t+1\rangle}$ is non-zero at i and zero over $S \setminus \{i\}$. Letting i vary we see that $C^{\langle t+1\rangle}$ has full rank over S, hence $\dim C^{\langle t+1\rangle} \geq k_t$. This is the first inequality.

Now let $d_t = \mathrm{d}_{\min}^{\langle t\rangle}(C)$ and let $c \in C^{\langle t\rangle}$ be a codeword of weight d_t. Let i be a non-zero coordinate of c, so by Lemma 10 we can find $c' \in C$ that is non-zero at i. Then $c * c' \in C^{\langle t+1\rangle}$ is non-zero at i, so it is not the zero codeword, and its support is a subset of the support of c, hence $\mathrm{d}_{\min}(C^{\langle t+1\rangle}) \leq d_t$. This is the second inequality. $\square$

Corollary 12. *Let $n \geq k \geq 1$ and $s \geq 0$ be integers, and let $N = (s+1)(2s+1)n$. Let also $\phi : \mathbb{F}_{q^{2s+1}} \longrightarrow (\mathbb{F}_q)^{(s+1)(2s+1)}$ be the $\mathbb{F}_q$-linear map defined earlier. Then, for any $\mathbb{F}_{q^{2s+1}}$-linear $[n, k]$ code C, the "concatenated" code $\phi(C)$ is a $\mathbb{F}_q$-linear code of length N, and we have:*

- *(i)* $\dim \phi(C) = (2s + 1) \dim C$
- *(ii)* $\mathrm{d}_{\min}^{\langle 2\rangle}(\phi(C)) \geq \mathrm{d}_{\min}^{\langle 1+\mathrm{q}^{\mathrm{s}}\rangle}(C)$
- *(iii)* $\mathrm{R}(\phi(C)) = \frac{1}{s+1}\, \mathrm{R}(C)$
- *(iv)* $\delta^{\langle 2\rangle}(\phi(C)) \geq \frac{1}{(s+1)(2s+1)}\, \delta^{\langle 1+\mathrm{q}^{\mathrm{s}}\rangle}(C)$

where, in the left, parameters (and coordinatewise product) are meant over $\mathbb{F}_q$, and in the right, they are over $\mathbb{F}_{q^{2s+1}}$.

Proof. Remark that ϕ is injective, since it was constructed by extending a basis $t_{\gamma_1}, \ldots, t_{\gamma_r}$ of $(\mathbb{F}_{q^r})^\vee$, where $r = 2s + 1$. This implies that $\phi(C)$ has dimension rk, from which (i) and (iii) follow.

On the other hand, since $m_0(x,y) = xy$ and $m_j(x,y) = xy^{q^j} + x^{q^j}y$ for $j \geq 1$, we find

$$\langle m_j(C,C)\rangle \subset C^{\langle 1+q^j\rangle}$$

for all $j \geq 0$. In this inclusion, the right-hand side is a $\mathbb{F}_{q^{2s+1}}$-linear code, while in general the left-hand side is only a $\mathbb{F}_q$-linear subspace. Nevertheless this implies

$$\mathrm{d_{min}}(\langle m_j(C,C)\rangle) \geq \mathrm{d}_{\mathrm{min}}^{\langle 1+\mathrm{q}^{\mathrm{j}}\rangle}(C)$$

and together with Propositions 8 and 11, this gives (ii), and then (iv). □

5 Algebraic-geometry codes

Let K be a finite field. If X is a (smooth, projective, absolutely irreducible) curve over K, we define a divisor D on X as a formal sum of (closed) points of X, to which one associates the K-vector space $L(D)$, of dimension $l(D)$, made of the functions f on X having poles at most D (where a pole of negative order means a zero of opposite order). We also define a degree function on the group of divisors by extending by linearity the degree function of points. It is then known:

- $l(D) = 0$ if $\deg(D) < 0$
- $l(D) \geq \deg(D) + 1 - g$ (Riemann's inequality)

where g is the genus of X (and Riemann's inequality can now be seen as part of the subsequent Riemann-Roch theorem).

If $G = P_1 + \cdots + P_n$ is a divisor that is the sum of n distinct degree 1 points of X, then, provided D and G have disjoint support, we can define an evaluation map

$$\begin{array}{rccc} \mathrm{ev}_{D,G}: & L(D) & \longrightarrow & K^n \\ & f & \mapsto & (f(P_1),\ldots,f(P_n)) \end{array}$$

and an evaluation code

$$C(D,G) \subset K^n$$

as the image of this K-linear map $\mathrm{ev}_{D,G}$. Then, from the preceding properties of $l(D)$ we deduce:

Lemma 13 (Goppa)**.** *Suppose $g \leq \deg(D) < n$. Then*

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

and

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

Evaluation codes also behave well with regard to our intersection span operations:

Lemma 14. *For any integer $t \geq 0$ we have*

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

Proof. This is true for $t = 0$, so by induction it suffices to show $\langle C(tD,G) * C(D,G)\rangle \subset C((t+1)D,G)$, or more generally,

$$\langle C(D,G) * C(D',G)\rangle \subset C(D+D',G)$$

for any divisors D, D' with supports disjoint from G. But for $c \in C(D,G)$ and $c' \in C(D',G)$, write $c = \mathrm{ev}(f)$ and $c' = \mathrm{ev}(f')$ with $f \in L(D)$ and $f' \in L(D')$, and then $c * c' = \mathrm{ev}(ff')$ with $ff' \in L(D+D')$, from which the conclusion follows. □

Proposition 15. *Let q be a prime power, and $s \geq 0$ an integer. Let X be a curve over $\mathbb{F}_{q^{2s+1}}$, of genus g, and suppose that X admits a set $\{P_1, \dots, P_n\}$ of degree 1 points of cardinality*

$$n > (1+q^s)g.$$

Let then $G = P_1 + \dots + P_n$. Let also D be a divisor on X of support disjoint from G and whose degree $\deg(D) = m$ satisfies

$$g \leq m < \frac{n}{1+q^s}.$$

Finally let

$$\phi : \mathbb{F}_{q^{2s+1}} \longrightarrow (\mathbb{F}_q)^{(s+1)(2s+1)}$$

as in the previous section. Then the corresponding concatenated code

$$C = \phi(C(D,G)) \subset (\mathbb{F}_q)^{(s+1)(2s+1)n}$$

has parameters satisfying:

(i) $\dim C \geq (2s+1)(m+1-g)$

(ii) $\mathrm{d}_{\min}^{\langle 2\rangle}(C) \geq n - (1+q^s)m$

(iii) $\mathrm{R}(C) \geq \dfrac{1}{s+1}\dfrac{m+1-g}{n}$

(iv) $\delta^{\langle 2\rangle}(C) \geq \dfrac{1}{(s+1)(2s+1)}\left(1 - \dfrac{(1+q^s)m}{n}\right)$

Proof. Inequalities (i) and (iii) follow from (i) and (iii) in Corollary 12 joint with Lemma 13.

Inequalities (ii) and (iv) follow from (ii) and (iv) in Corollary 12 joint with Lemma 13 applied to $C((1+q^s)D,G)$ and Lemma 14 applied with $t = 1+q^s$. □

For any prime power q, let $N_q(g)$ be the maximal possible number of degree 1 points of a curve of genus g over $\mathbb{F}_q$, and let

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

We will now make use of a recent result of Garcia-Stichtenoth-Bassa-Beelen [7], in the following form:

Lemma 16. *For any prime power q, there exists an integer s such that*

$$A(q^{2s+1}) > 1 + q^s$$

(and in fact this holds as soon as s is large enough).

Proof. If q is a square, one knows from [8] that $A(q^{2s+1}) \geq (q^{2s+1})^{1/2} - 1 > 1 + q^s$ as soon as s is large enough. So suppose q is not a square, say $q = p^{2t+1}$ with p prime. Then Theorem 1.1 of [7] gives

$$A(q^{2s+1}) = A(p^{4st+2s+2t+1}) \geq \frac{2(p^{2st+s+t+1} - 1)}{p + 1 + \varepsilon_s}$$

with $\varepsilon_s \to 0$ as $s \to \infty$, so, for s large enough, this is greater than

$$1 + q^s = 1 + p^{2st+s}$$

as claimed. $\square$

From this we can finally prove our main theorem.

Theorem 17. *Let q be a prime power, and let s be as given by Lemma 16. Then, for any real number μ with*

$$1 < \mu < \frac{A(q^{2s+1})}{1 + q^s}$$

there exists a family of linear codes C_i over $\mathbb{F}_q$, of length going to infinity, satisfying

$$\liminf_{i\to\infty} \mathrm{R}(C_i) \geq \frac{1}{s+1} \frac{\mu - 1}{A(q^{2s+1})}$$

and

$$\liminf_{i\to\infty} \delta^{\langle 2\rangle}(C_i) \geq \frac{1}{(s+1)(2s+1)} \left(1 - \frac{(1+q^s)\mu}{A(q^{2s+1})}\right).$$

Proof. For any curve X over $\mathbb{F}_{q^{2s+1}}$, denote by $N(X)$ the number of its degree 1 points. Let X_i be a sequence of curves of genus g_i going to infinity, and such that $\lim_i \frac{N(X_i)}{g_i} = A(q^{2s+1})$. Also choose a sequence of integers m_i such that $\lim_i \frac{m_i}{g_i} = \mu$.

Now, given i large enough, write $n_i = N(X_i) - 1$, let $P_{i,0}, P_{i,1}, \ldots, P_{i,n_i}$ be the degree 1 points of X_i, and let $D_i = m_i P_{i,0}$. Then Proposition 15 gives a code C_i over $\mathbb{F}_q$ of length $(s+1)(2s+1)n_i$ with $\mathrm{R}(C_i) \geq \frac{1}{s+1}\frac{m_i+1-g_i}{n_i}$ and $\delta^{\langle 2\rangle}(C_i) \geq \frac{1}{(s+1)(2s+1)}\left(1 - \frac{(1+q^s)m_i}{n_i}\right)$, and the conclusion follows. $\square$

Remark that the proof of Theorem 17 is constructive, and works also for a possibly non-optimal sequence of curves over $\mathbb{F}_{q^{2s+1}}$, by which we mean, curves satisfying $\liminf_i \frac{N(X_i)}{g_i} \geq A'$ for a certain $A' \leq A(q^{2s+1})$, provided still $A' > 1 + q^s$ and one replaces all occurences of $A(q^{2s+1})$ in the theorem with A'.

For example [7] gives an explicit sequence of curves over $\mathbb{F}_{2^9}$ with $\lim_i \frac{N(X_i)}{g_i} \geq A' = 465/23 \approx 20.217 > 17 = 1 + 2^4$. Choosing $\mu = 186/161$ then gives an explicit sequence of binary linear codes C_i of length going to infinity with $\liminf_i \mathrm{R}(C_i) \geq 1/651$ and $\liminf_i \delta^{\langle 2\rangle}(C_i) \geq 1/1575$. Of course these are only lower bounds, and it could well be that these codes actually have much better parameters.

6 Concluding remarks and open problems

Keeping Proposition 11 in mind, perhaps the most general question one can ask about the parameters of successive powers of codes is the following: given a prime power q, an integer n, and two sequences $k_1 \leq k_2 \leq k_3 \leq \dots$ and $d_1 \geq d_2 \geq d_3 \geq \dots$, does there exist a linear code $C \subset (\mathbb{F}_q)^n$ with $\dim^{\langle \mathrm{t}\rangle}(C) = k_t$ and $\mathrm{d}_{\min}^{\langle \mathrm{t}\rangle}(C) = d_t$ for all t? In fact, already of interest is the study of the function

$$a_q^{\langle t\rangle}(n,d) = \max\{k \geq 0 \,|\, \exists C \subset (\mathbb{F}_q)^n,\ \dim(C) = k,\ \mathrm{d}_{\min}^{\langle \mathrm{t}\rangle}(C) \geq d\}.$$

Proposition 11 gives $a_q^{\langle t\rangle}(n,d) \geq a_q^{\langle t+1\rangle}(n,d)$, and Corollary 12 gives

$$a_q^{\langle 2\rangle}((s+1)(2s+1)n,d) \geq (2s+1)a_{q^{2s+1}}^{\langle 1+q^s\rangle}(n,d)$$

for all $s \geq 0$.

But besides parameters, one can ask for other characterizations of codes that are powers. Consider for example the "square root" problem: given a linear code $C \subset (\mathbb{F}_q)^n$, can one decide if there exists a code C_0 such that $C = C_0^{\langle 2\rangle}$, and if so, how many are there? can one construct one such square root, or all of them, effectively?

An obvious counting argument shows that, on average, a code taken randomly in the set of all codes of given length admits one square root. However the actual distribution of squares within the set of codes of given parameters might be quite inhomogeneous, and would be interesting to study. For example, all binary codes of length 3, except two of them, are their own unique square root. The two exceptions are: the $[3,2,2]$ parity code is not a square; the trivial $[3,3,1]$ code admits two square roots, namely itself and the $[3,2,2]$ code.

Now we turn to asymptotic properties. Define

$$\alpha_q^{\langle t\rangle}(\delta) = \limsup_{n\to\infty} \frac{a_q^{\langle t\rangle}(n,\lfloor \delta n\rfloor)}{n},$$

$$\delta_q(t) = \sup\{\delta \geq 0 \,|\, \alpha_q^{\langle t\rangle}(\delta) > 0\},$$

and

$$\tau(q) = \sup\{t \in \mathbb{N} \mid \delta_q(t) > 0\}.$$

That is, $\tau(q)$ is the supremum value (possibly $+\infty$) of t such that there exists an asymptotically good family of linear codes C_i over $\mathbb{F}_q$ whose t-th powers $C_i^{\langle t\rangle}$ also form an asymptotically good family.

From Corollary 12 one finds

$$\alpha_q^{\langle 2\rangle}(\delta) \geq \frac{1}{s+1}\alpha_{q^{2s+1}}^{\langle 1+q^s\rangle}((s+1)(2s+1)\delta)$$

and

$$\delta_q(2) \geq \frac{1}{(s+1)(2s+1)}\delta_{q^{2s+1}}(1+q^s)$$

for all $s \geq 0$.

On the other hand, from Lemma 13 and Lemma 14 one easily finds

$$\alpha_q^{\langle t\rangle}(\delta) \geq \frac{1-\delta}{t} - \frac{1}{A(q)}$$

and

$$\delta_q(t) \geq 1 - \frac{t}{A(q)}$$

hence

$$\tau(q) \geq \lceil A(q)\rceil - 1$$

(which is non-trivial only for q large).

Combining these bounds, or equivalently, eliminating μ from the two estimates in Theorem 17, one gets

$$\alpha_q^{\langle 2\rangle}(\delta) \geq \frac{1}{s+1}\left(\frac{1}{1+q^s} - \frac{1}{A(q^{2s+1})}\right) - \frac{2s+1}{1+q^s}\,\delta$$

and

$$\delta_q(2) \geq \frac{1}{(s+1)(2s+1)}\left(1 - \frac{1+q^s}{A(q^{2s+1})}\right)$$

for all $s \geq 0$, and hence, by Lemma 16,

$$\tau(q) \geq 2$$

for all q (which was precisely Theorem 1).

When $q = p$ is prime, these estimates can be made more precise using the bound $\frac{1}{A(p^{2s+1})} \leq \frac{1}{2}\left(\frac{1}{p^s-1} + \frac{1}{p^{s+1}-1}\right)$ from [7]. For $p = 2$, the best choice is $s = 4$, which gives

$$\alpha_2^{\langle 2\rangle}(\delta) \geq \frac{74}{39525} - \frac{9}{17}\,\delta \;\approx\; 0.001872 - 0.5294\,\delta$$

and

$$\delta_2(2) \geq \frac{74}{20925} \approx 0.003536.$$

This can be viewed as a quantitative version of the claim $\tau(2) \geq 2$ made in the title of this article. However, in the other direction, the author doesn't know any upper bound on the $\tau(q)$, for instance, he doesn't even know whether $\tau(2)$ is finite.

References

[1] S. Ballet and J. Pieltant, "On the tensor rank of multiplication in any extension of $\mathbb{F}_2$", J. Complexity, Vol. 27, pp. 230-245, 2011.

[2] I. Cascudo, H. Chen, R. Cramer, and C. Xing, "Asymptotically good ideal linear secret sharing with strong multiplication over any fixed finite field", in *Advances in Cryptology — CRYPTO 2009* (Lecture Notes in Comp. Science, Vol. 5677), S. Halevi, Ed. Berlin: Springer-Verlag, 2009, pp. 466-486.

[3] I. Cascudo, R. Cramer, and C. Xing, "The torsion-limit for algebraic function fields and its application to arithmetic secret sharing", in *Advances in Cryptology — CRYPTO 2011* (Lecture Notes in Comp. Science, Vol. 6841), P. Rogaway, Ed. Berlin: Springer-Verlag, 2011, pp. 685-705.

[4] I. Cascudo, R. Cramer, C. Xing, and A. Yang, "Asymptotic bound for multiplication complexity in the extensions of small finite fields", *IEEE Trans. Inform. Theory*, Vol. 58, pp. 4930-4935, July 2012.

[5] G. Cohen and A. Lempel, "Linear intersecting codes", *Discr. Math.*, Vol. 56, pp. 35-43, 1985.

[6] V. Drinfeld and S. Vladut, "Number of points of an algebraic curve", Funct. Anal., Vol. 17, pp. 53-54, 1983.

[7] A. Garcia, H. Stichtenoth, A. Bassa, and P. Beelen, "Towers of function fields over non-prime finite fields", to be published. Available: `http://arxiv.org/abs/1202.5922`

[8] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, Vol. 28, pp. 721-724, 1981.

[9] A. Lempel and S. Winograd, "A new approach to error-correcting codes", *IEEE Trans. Inform. Theory*, Vol. 23, pp. 503-508, July 1977.

[10] D. Miklós, "Linear binary codes with intersection properties", *Discr. Appl. Math.*, Vol. 9, pp. 187-196, 1984.

[11] H. Randriambololona, "Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method", J. Complexity, Vol. 28, pp. 489-517, 2012.

[12] H. Randriambololona, "$(2, 1)$-separating systems beyond the probabilistic bound", *Israel J. Math.*, to be published. Available: `http://arxiv.org/abs/1010.5764`

[13] C. Xing, "Asymptotic bounds on frameproof codes", *IEEE Trans. Inform. Theory*, Vol. 48, pp. 2991-2995, Nov. 2002.