An upper bound of Singleton type for componentwise products of linear codes

Hugues Randriambololona

September 5, 2013

Abstract

We give an upper bound that relates the dimensions of some given number of linear codes, with the minimum distance of their componentwise product. A typical result is as follows: given t linear codes C_i of parameters $[n, k_i]_q$ with full support, one can find codewords $c_i \in C_i$ such that $1 \leq w(c_1 * \cdots * c_t) \leq \max(t-1,\, n+t-(k_1+\cdots+k_t)\,)$.

1 Introduction

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

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

If $C_1, \ldots, C_t \subseteq (\mathbb{F}_q)^n$ are linear codes of the same length n, let

$$C_1 * \cdots * C_t = \sum_{c_i \in C_i} \mathbb{F}_q \cdot c_1 * \cdots * c_t \ \subseteq \ (\mathbb{F}_q)^n$$

be the linear code spanned by the componentwise products of their codewords. (In [8] this was denoted $\langle C_1 * \cdots * C_t \rangle$ with brackets meant to emphasize that the linear span is taken. Here we will keep notation lighter. All codes in this text will be linear.)

Also define the square of a linear code C as the linear code $C^{\langle 2 \rangle} = C * C$, and likewise for its higher powers $C^{\langle t \rangle}$.

Basic properties of these operations, as well as a geometric interpretation, will be found in [9].

Bounds on the possible joint parameters of C and $C^{\langle t \rangle}$, or more generally on that of some C_i and their product $C_1 * \cdots * C_t$, have attracted attention recently for various reasons:

- they determine the performance of bilinear multiplication algorithms, in particular against random or adversarial errors, or against eavesdropping; this is useful either in questions of algebraic complexity [4][7], or in the study of secure multi-party computation systems [1]
- since $C_1 * \cdots * C_t$ captures possibly hidden algebraic relations between subcodes C_i of a larger code (given by an apparently random generator matrix), they're at the heart of attacks [2] against McEliece type cryptosystems

- following [10], the existence of asymptotically good binary linear codes with asymptotically good squares is the key ingredient in an improvement of the Crépeau-Kilian [3] oblivious transfer protocol over a noisy channel; solving this problem was the main motivation for [8]
- last, this $*$ operation is also of use in the understanding of algebraic decoding algorithms through the notion of error-locating pairs [6].

While it is possible to give bounds involving subtler parameters, such as the dual distance (see Lemma 6 below for an elementary example, or [5] for a more elaborate result), here we want to deal with "clean" bounds involving only the dimensions of the C_i and the minimum distance of $C_1 * \cdots * C_t$. In particular we will study the following generalizations (introduced in [8]) of the fundamental functions of block coding theory:

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

and

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

In fact, for $t \geq 2$ we have the easy inequalities $\dim(C^{\langle t \rangle}) \geq \dim(C^{\langle t-1 \rangle})$ and $\mathrm{d}_{\min}(C^{\langle t \rangle}) \leq \mathrm{d}_{\min}(C^{\langle t-1 \rangle})$ (see [8], Prop. 11), from which one deduces

$$a_q^{\langle t \rangle}(n,d) \leq a_q^{\langle t-1 \rangle}(n,d) \leq \cdots \leq a_q(n,d)$$

$$\alpha_q^{\langle t \rangle}(\delta) \leq \alpha_q^{\langle t-1 \rangle}(\delta) \leq \cdots \leq \alpha_q(\delta)$$

where $a_q(n,d)$, $\alpha_q(\delta)$, are the usual, much-studied fundamental functions; hence all the upper bounds known on these functions apply. Here we will get a new, stronger bound, by working directly on the generalized functions.

The paper is organized as follows. In Section 2 we state and prove our main result, the product Singleton bound, in full generality. In Section 3 we propose an alternative proof that works only in a special case, and moreover leads to a slightly weaker result; but it uses entirely different methods that could be of independent interest. Then in Section 4 we derive our new upper bound on the fundamental functions; in particular for $d \leq t$ we get the exact value of $a_q^{\langle t \rangle}(n,d)$.

Notations. We let $[n] = \{1, \ldots, n\}$ be the standard set with n elements. Given a subset $I \subseteq [n]$, we let $\pi_I : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^I$ be the natural projection.

2 The product Singleton bound

Here we state our main result, which for $t = 1$ reduces to the (linear version of the) classical Singleton bound. For this we introduce a mild technical condition (which will be discussed further in Remark 3 below).

Definition 1. *Let $t \geq 3$ be an integer and let $C_1, \ldots, C_t \subseteq (\mathbb{F}_q)^n$ be linear codes of the same length n. We say these C_i satisfy the* support condition *if, for each coordinate $j \in [n]$, either j is in the support of* all *the C_i, or it is in the support of* at most one *of them.*

Theorem 2. *Let $t \geq 1$ be an integer and let $C_1, \ldots, C_t \subseteq (\mathbb{F}_q)^n$ be linear codes of dimension $k_1, \ldots, k_t$ respectively, and of the same length n. Suppose $C_1 * \cdots * C_t \neq 0$, and if $t \geq 3$ suppose they satisfy the* support condition. *Then one can find codewords $c_i \in C_i$ such that their product $c_1 * \cdots * c_t$ has weight*

$$1 \leq w(c_1 * \cdots * c_t) \leq \max(t-1,\, n + t - (k_1 + \cdots + k_t)\,).$$

As a consequence, $\mathrm{d}_{\min}(C_1 * \cdots * C_t) \leq \max(t-1,\, n + t - (k_1 + \cdots + k_t)\,)$.

This upper bound is tight. For example it is attained when the C_i are Reed-Solomon codes, with $k_1 + \cdots + k_t \leq n$.

Also when $k_1 + \cdots + k_t > n$, the upper bound $t-1$ can be attained. For an example with $t = 3$ consider the code C with generator matrix $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$. Then $tk = 6 > n = 4$, and $C^{\langle 3 \rangle} = C$ has $\mathrm{d}_{\min} = t - 1 = 2$.

Note that the existence of the c_i is stronger than the bound on the minimum distance alone: indeed, in general $\mathrm{d}_{\min}(C_1 * \cdots * C_t)$ need not be attained by a codeword z in specific product form $z = c_1 * \cdots * c_t$ (one might need *a linear combination* of such codewords). However, what makes the proof difficult is that, while we want the intersection of the supports of the c_i to be small, at the same time we need to ensure it remains nonempty.

Remark 3. Here we want to make a few comments about the *support condition*:

(a) Although this *support condition* for $t \geq 3$ might seem a little bit restrictive, in fact it is satisfied in many important situations. For instance, it is satisfied when $C_1, \ldots, C_t$ all have full support, or when $C_1 = \cdots = C_t = C$ are all equal to the same code C (not necessarily of full support).

(b) However, the conclusion in Theorem 2 can fail if one drops the *support condition*. For example, the codes C_1, C_2, C_3 with generator matrices $G_1 = G_2 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $G_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \end{pmatrix}$ have $k_1 + k_2 + k_3 = 5 > n = 4$, but $\mathrm{d}_{\min}(C_1 * C_2 * C_3) = 3$.

(c) Here we assume that we have a proof of Theorem 2 in the particular case where all C_i have full support.

First, this allows us to deduce the following *unconditional* variant:

Let $C_1, \ldots, C_t \subseteq (\mathbb{F}_q)^n$ be *any* linear codes of the same length n. Suppose $I = \bigcap_i \mathrm{Supp}(C_i) \neq \emptyset$, and let $\overline{n} = |I|$, $\overline{k}_i = \dim \pi_I(C_i)$. Then one can find codewords $c_i \in C_i$ such that their product has weight

$$1 \leq w(c_1 * \cdots * c_t) \leq \max(t-1,\, \overline{n} + t - (\overline{k}_1 + \cdots + \overline{k}_t)\,).$$

Indeed, the codes $\pi_I(C_i)$ all have full support in I, so by our assumption one can find codewords $\pi_I(c_i) \in \pi_I(C_i)$ satisfying the estimates. Then just observe that $w(c_1 * \cdots * c_t) = w(\pi_I(c_1) * \cdots * \pi_I(c_t))$.

Now we claim that, in turn, this implies the full statement of Theorem 2. Indeed suppose the C_i satisfy the *support condition* if $t \geq 3$. Write $\mathrm{Supp}(C_i) = I \cup J_i$. The J_i are disjoint: this is obvious if $t \leq 2$, and if $t \geq 3$ this is precisely

the meaning of the *support condition*. Then we have $\overline{n} \leq n-(|J_1|+\cdots+|J_t|)$, while $\overline{k}_i \geq k_i - |J_i|$, hence

$$\overline{n} + t - (\overline{k}_1 + \cdots + \overline{k}_t) \leq n + t - (k_1 + \cdots + k_t)$$

which finishes the proof.

Thanks to the equivalence of the statements in the last remark, we see that to prove Theorem 2, it suffices to do so under the additional assumption that all the codes have full support. The key step in the proof will be the following lemma, which treats the case of "high dimension".

Lemma 4. *Let $C_1, \ldots, C_t \subseteq (\mathbb{F}_q)^n$ be linear codes of dimension $k_1, \ldots, k_t$ respectively, and of the same length n. Suppose these codes all have full support, and*

$$k_1 + \cdots + k_t > n.$$

Then one can find codewords $c_i \in C_i$ such that

$$1 \leq w(c_1 * \cdots * c_t) \leq t - 1.$$

Proof. If H is a matrix with n columns, we say that a subset $A \subseteq [n]$ is dependent (resp. independent, maximal independent) in H if, in the set of columns of H, those indexed by A form a linearly dependent (resp. independent, maximal independent) family.

Now let H_i be a parity-check matrix for C_i. We claim that we can find subsets $A_1, \ldots, A_t \subseteq [n]$, and an element $j_1 \in [n]$, such that:

(1) $A_1 \cap \cdots \cap A_t = \emptyset$

(2) A_1 is independent in H_1

(3) A_i is maximal independent in H_i for $i \geq 2$

(4) $A_1 \cup \{j_1\}$ is dependent in H_1, and $A_2 \cup \{j_1\}$ is dependent in H_2.

These are constructed as follows. First, for all i, choose any $B_i \subseteq [n]$ maximal independent in H_i, and let $I = B_1 \cap \cdots \cap B_t$ be their intersection. Then $|B_1| + \cdots + |B_t| = tn - (k_1 + \cdots + k_t) < (t-1)n$, so there exists $j_1 \in [n]$ that belongs to at most $t-2$ of the sets B_i. Say $j_1 \notin B_1$ and $j_1 \notin B_2$.

Suppose $(B_1 \setminus I) \cup \{j_1\}$ is independent in H_1. Then I is nonempty (otherwise B_1 would not be maximal), and by the basis exchange property from elementary linear algebra, one can find $j \in I$ such that $(B_1 \setminus \{j\}) \cup \{j_1\}$ is maximal independent in H_1. Then we replace B_1 with $(B_1 \setminus \{j\}) \cup \{j_1\}$, which replaces I with $I \setminus \{j\}$.

We repeat this procedure until, obviously, it must stop, which means $(B_1 \setminus I) \cup \{j_1\}$ is dependent in H_1. Then we set $A_1 = B_1 \setminus I$, and $A_i = B_i$ for $i \geq 2$.

Now that this is done, by (2) and (4) there is $c_1 \in C_1$ with

$$\{j_1\} \subseteq \mathrm{Supp}(c_1) \subseteq A_1 \cup \{j_1\},$$

and likewise by (3) and (4) there is $c_2 \in C_2$ with

$$\{j_1\} \subseteq \mathrm{Supp}(c_2) \subseteq A_2 \cup \{j_1\},$$

hence

$$\{j_1\} \subseteq \mathrm{Supp}(c_1 * c_2) \subseteq (A_1 \cap A_2) \cup \{j_1\}.$$

This means we have established the step $s = 2$ in the following induction procedure:

Suppose for some $s \leq t$ we have found indices $j_1, \ldots, j_{s-1} \in [n]$ (not necessarily distinct) and codewords $c_1 \in C_1, \ldots, c_s \in C_s$ (after possibly renumbering), such that:

$$(5) \quad \{j_{s-1}\} \subseteq \mathrm{Supp}(c_1 * \cdots * c_s) \subseteq (A_1 \cap \cdots \cap A_s) \cup \{j_1, \ldots, j_{s-1}\}.$$

If $s = t$, the proof is finished thanks to condition (1). So we suppose $s < t$, and we will show how to pass from s to $s + 1$ in the induction.

By (5) we can write

$$\mathrm{Supp}(c_1 * \cdots * c_s) = S \cup T$$

with

$$S \subseteq A_1 \cap \cdots \cap A_s$$

and

$$\{j_{s-1}\} \subseteq T \subseteq \{j_1, \ldots, j_{s-1}\}.$$

We distinguish two cases.

First, suppose $S = \emptyset$. Set $j_s = j_{s-1}$. Then we can find $c_{s+1} \in C_{s+1}$ nonzero at j_s (because C_{s+1} has full support), and we're done.

Otherwise, suppose $S \neq \emptyset$, so there is $j_s \in S$. By (1), there is $i > s$ such that $j_s \notin A_i$. Say this is $i = s + 1$. Then, by (3), one can find $c_{s+1} \in C_{s+1}$ such that

$$\{j_s\} \subseteq \mathrm{Supp}(c_{s+1}) \subseteq A_{s+1} \cup \{j_s\},$$

from which it follows

$$\{j_s\} \subseteq \mathrm{Supp}(c_1 * \cdots * c_{s+1}) \subseteq (A_1 \cap \cdots \cap A_{s+1}) \cup \{j_1, \ldots, j_s\}.$$

The proof is complete. □

End of the proof of Theorem 2. Thanks to Remark 3(c) we can assume all C_i have full support. Also we assume $k_1 + \cdots + k_t \leq n$, otherwise it suffices to apply Lemma 4.

We conclude with the same puncturing argument as in one of the proofs of the classical Singleton bound: let π denote projection on the first $(k_1 + \cdots + k_t) - 1$ coordinates. We distinguish two cases.

First, suppose $\dim(\pi(C_i)) = \dim(C_i) = k_i$ for all i. Then we can apply Lemma 4 and we get $\pi(c_i) \in \pi(C_i)$ such that $1 \leq w(\pi(c_1) * \cdots * \pi(c_t)) \leq t - 1$. Lifting back we find $1 \leq w(c_1 * \cdots * c_t) \leq n + t - (k_1 + \cdots + k_t)$, which finishes the proof.

Otherwise, if this fails say for $i = 1$, there is $c_1 \in C_1$ nonzero in $\ker(\pi)$, so $w(c_1) \leq n + 1 - (k_1 + \cdots + k_t)$. Fix a coordinate $j \in \mathrm{Supp}(c_1)$ and for each $i \geq 2$ take $c_i \in C_i$ nonzero at j (which is possible since C_i has full support). Then $c_1 * \cdots * c_t$ is nonzero with weight $w(c_1 * \cdots * c_t) \leq w(c_1) \leq n + 1 - (k_1 + \cdots + k_t) \leq n + t - (k_1 + \cdots + k_t)$, as needed. □

Observe that our proof of Theorem 2 is constructive: $c_1, \ldots, c_t$ can be effectively computed from given parity-check matrices of the codes.

3 An alternative proof for $t = 2$

Consider the following statement, that is easily seen to be a special case of Theorem 2.

Proposition 5. *Let $C, C' \subseteq (\mathbb{F}_q)^n$ be linear codes of dimension k, k' respectively, and of the same length n. Then their product $C * C'$ has minimum distance*

$$\mathrm{d}_{\min}(C * C') \leq \max(1, n - k - k' + 2).$$

Compared with Theorem 2, an obvious restriction is that we consider the product of only $t = 2$ codes. But Proposition 5 is also less precise: given $C * C' \neq 0$, it says there is a nonzero codeword z of weight at most $\max(1, n-k-k'+2)$, but it does not give any information on it; while from Theorem 2, we know it can be taken in elementary product form $z = c * c'$ (and moreover it can be effectively computed).

However Proposition 5 can be proved using entirely different methods. For this we will need two lemmas.

Lemma 6. *Let $C_1, C_2 \subseteq (\mathbb{F}_q)^n$ be two linear codes. Suppose both C_1, C_2 have dual minimum distance at least* 2, i.e. *full support. Then:*

$$\dim(C_1 * C_2) \geq \min(n,\, \dim(C_1) + \mathrm{d}_{\min}(C_2^{\perp}) - 2).$$

Proof. Set $k_1 = \dim(C_1)$, $d_2^{\perp} = \mathrm{d}_{\min}(C_2^{\perp})$, and $m = \min(n, k_1 + d_2^{\perp} - 2)$. Then $m - k_1 + 1 \leq d_2^{\perp} - 1$, so any $m - k_1 + 1$ columns of C_2 are linearly independent, in particular:

Fact. For any set of indices $J \subseteq [n]$ of size $|J| = m - k_1$, and for any $j_0 \notin J$, there is a codeword $y \in C_2$ with $y_{j_0} = 1$ and $y_j = 0$ for $j \in J$.

Now (after possibly permuting coordinates) put C_1 in systematic form, with generator matrix $G_1 = (I_{k_1} | X)$. To show $\dim(C_1 * C_2) \geq m$, we will find, for each $i \in [m]$, a codeword $z \in C_1 * C_2$ with $z_i \neq 0$ and $z_j = 0$ for $j \in [m] \setminus \{i\}$. We distinguish two cases.

First, suppose $i \in [k_1]$. Let x be the i-th row of G_1, and let y be given by the Fact with $j_0 = i$ and $J = [m] \setminus [k_1]$. Then we can set $z = x * y$.

Otherwise, suppose $i \in [m] \setminus [k_1]$. Since C_1 has full support, there is a row of G_1 that is nonzero at i. Say this is the i'-th row, and denote it by x. Now let y be given by the Fact with $j_0 = i$ and $J = \{i'\} \cup ([m] \setminus ([k_1] \cup \{i\}))$. Then again $z = x * y$ does the job. □

Lemma 7. *For any two linear codes $C, C' \subseteq (\mathbb{F}_q)^n$ we have*

$$C \;\perp\; C' * (C * C')^{\perp}.$$

Proof. Let $\tau : (\mathbb{F}_q)^n \to \mathbb{F}_q$ be the "trace" linear map, $\tau(x_1, \ldots, x_n) = x_1 + \cdots + x_n$. Note that the canonical scalar product $\langle \cdot | \cdot \rangle$ on $(\mathbb{F}_q)^n$ can be written as $\langle c | c' \rangle = \tau(c * c')$. Now for any $c \in C$, $c' \in C'$, and $x \in (C * C')^{\perp}$, we have

$$\langle c | c' * x \rangle = \tau(c * (c' * x)) = \tau((c * c') * x) = \langle c * c' | x \rangle = 0$$

and we conclude by passing to the linear span. □

We can now proceed. In what follows let $\widetilde{d} = \mathrm{d}_{\min}(C * C')$.

Proof of Proposition 5. It suffices to treat the case where C and C' both have full support. For then, to deduce the case of general C and C', just project on the intersection of their supports: this leaves $\widetilde{d}$ unchanged, while $n-k-k'$ can only decrease (this is the very same argument as in Remark 3(c)).

Also suppose $\widetilde{d} \geq 2$, otherwise there is nothing to prove.

That C has full support implies that for any $c' \in C'$ of minimum weight $d' = \mathrm{d}_{\min}(C')$, there is a $c \in C$ whose support intersects that of c' non-trivially, meaning $c * c' \neq 0$: this implies $\widetilde{d} \leq d'$, hence by the classical Singleton bound

$$k' \leq n - \widetilde{d} + 1.$$

Lemma 6 applied with $C_1 = C'$ and $C_2 = (C * C')^{\perp}$ then gives

$$\dim(C' * (C * C')^{\perp}) \geq k' + \widetilde{d} - 2,$$

and by Lemma 7 we conclude

$$k \leq n - \dim(C' * (C * C')^{\perp}) \leq n - k' - \widetilde{d} + 2$$

as needed. □

In the author's opinion, Lemmas 6 and 7 are very natural and have interest on their own. But the way they combine to give this concise but not-so-intuitive proof of Proposition 5 is quite intriguing.

4 Upper bound on the generalized fundamental functions

An important consequence of Theorem 2 is the following:

Theorem 8. *We have* $a_q^{\langle t \rangle}(n,d) = \left\lfloor \frac{n}{d} \right\rfloor$ *for* $1 \leq d \leq t$, *and*

$$a_q^{\langle t \rangle}(n,d) \leq \left\lfloor \frac{n-d}{t} \right\rfloor + 1 \qquad \text{for } t < d \leq n.$$

Likewise, $\alpha_q^{\langle t \rangle}(0) = 1$, *and*

$$\alpha_q^{\langle t \rangle}(\delta) \leq \frac{1-\delta}{t} \qquad \text{for } 0 < \delta \leq 1.$$

Proof. Suppose first $d \geq t$. If C has parameters $[n,k]$ and $\mathrm{d}_{\min}(C^{\langle t \rangle}) \geq d$, Theorem 2 applied with all $C_i = C$ gives $d \leq n - (k-1)t$, from which the bound $a_q^{\langle t \rangle}(n,d) \leq \left\lfloor \frac{n-d}{t} \right\rfloor + 1$ follows.

In particular, on the "diagonal" $d = t$ we find $a_q^{\langle t \rangle}(n,t) \leq \left\lfloor \frac{n-t}{t} \right\rfloor + 1 = \left\lfloor \frac{n}{t} \right\rfloor$ for all t.

Then for $d < t$, we deduce $a_q^{\langle t \rangle}(n,d) \leq a_q^{\langle d \rangle}(n,d) \leq \left\lfloor \frac{n}{d} \right\rfloor$.

To show that this upper bound is in fact an equality for $d \leq t$, partition the set $[n]$ of coordinates into $\left\lfloor \frac{n}{d} \right\rfloor$ subsets of size d or $d+1$, and consider the code C spanned by their characteristic vectors (observe $C^{\langle t \rangle} = C$).

This done, letting $n \to \infty$ and normalizing then gives the estimate on $\alpha_q^{\langle t \rangle}(\delta)$. (For the special value $\alpha_q^{\langle t \rangle}(0) = 1$, we used $a_q^{\langle t \rangle}(n,1) = n$.) □

Note in particular that for $t \geq 2$, the function $\alpha_q^{\langle t \rangle}(\delta)$ is not continuous at $\delta = 0$, in striking contrast with the "usual" function $\alpha_q(\delta)$. Perhaps one could modify the definition of $\alpha_q^{\langle t \rangle}$ to remove this discontinuity. Nevertheless it remains $\limsup \alpha_q^{\langle t \rangle}(\delta) \leq \frac{1}{t} < 1$ as $\delta \to 0$. Thus for small δ our bound clearly improves on the inequality $\alpha_q^{\langle t \rangle}(\delta) \leq \alpha_q(\delta)$, and in fact one can show it is so for all $\delta < 1 - \varepsilon(q)$, with $\varepsilon(q) \to 0$ as $q \to \infty$.

Conversely it is interesting to compare the upper bound in Theorem 8 with known lower bounds. From algebraic-geometry codes one easily gets (see [8] for more details)

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

where $A(q)$ is the Ihara constant. When $q \to \infty$, the two bounds match. On the other hand, for q small, the two bounds remain far apart. For $t = 2$, even with the improved lower bound of [8], namely

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

(for any $s \geq 0$), there remains much room for progress. For instance, for $q = 2$, the best we get ($s = 4$) is

$$0.001872 - 0.5294\,\delta \;\leq\; \alpha_2^{\langle 2 \rangle}(\delta) \;\leq\; 0.5 - 0.5\,\delta.$$

Still for q small, the situation for $t \geq 3$ is even worse: no nontrivial lower bound on $\alpha_q^{\langle t \rangle}$ is known then!

Acknowledgment

The author is indebted to the Associate Editor Dr. Navin Kashyap for his proof of the case $t = 2$ of what is now Lemma 4. This was the key starting point in a series of improvements that led from Proposition 5 (which the author had beforehand) to the now much more general Theorem 2.

References

[1] 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.

[2] A. Couvreur, P. Gaborit, V. Gauthier, A. Otmani, and J.-P. Tillich. "Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes", *WCC 2013, International Workshop on Coding and Cryptography, Bergen, Norway*, Apr. 15-19, 2013. To appear.

[3] C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *Proc. 29th IEEE Symp. on Found. of Computer Sci. (FOCS '88)*, pp. 42-52, 1988.

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

[5] D. Mirandola, "Schur products of linear codes: a study of parameters", Master Thesis (under the supervision of G. Zémor), Univ. Bordeaux 1 and Stellenbosch Univ., July 2012. Available: `http://www.algant.eu/documents/theses/mirandola.pdf`

[6] R. Pellikaan, "On decoding by error location and dependent sets of error positions", *Discrete Math.*, Vol. 106/107, pp. 369-381, 1992.

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

[8] H. Randriambololona, "Asymptotically good binary linear codes with asymptotically good self-intersection spans", *IEEE Trans. Inform. Theory*, Vol. 59, pp. 3038-3045, May 2013.

[9] H. Randriambololona, "On products and powers of linear codes under componentwise multiplication", *Proc. 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT-14), Luminy, France*, June 3-7, 2013. To appear.

[10] G. Zémor. "(More) efficient oblivious transfer from noisy channels", Talk at DIAMANT Symposium, Doorn, Netherlands, Nov. 2012. Joint work with F. Oggier, article in preparation.