Advances in Mathematics of Communications
Volume 10, No. 1, 2016, 53–61
doi:10.3934/amc.2016.10.53

YET ANOTHER VARIATION ON MINIMAL LINEAR CODES

Gérard Cohen

Télécom ParisTech, UMR 5141, CNRS
46 rue Barrault, 75634 Paris Cedex 13, France

Sihem Mesnager

University of Paris XIII and Paris VIII, Télécom ParisTech
LAGA, UMR 7539, CNRS, Sorbonne Paris Cité, France

Hugues Randriam

Télécom ParisTech, UMR 5141, CNRS
46 rue Barrault, 75634 Paris Cedex 13, France

(Communicated by Raquel Pinto)

Abstract. Minimal linear codes are linear codes such that the support of every codeword does not contain the support of another linearly independent codeword. Such codes have applications in cryptography, e.g. to secret sharing. We pursue here their study and construct improved asymptotically good families of minimal linear codes. We also consider quasi-minimal, t-minimal, and t-quasi-minimal linear codes, which are new variations on this notion.

1. Introduction

A *minimal codeword* c of a linear code C is a codeword such that its support (set of non-zero coordinates) does not contain the support of another linearly independent codeword. Minimal codewords are useful for defining access structures in secret sharing schemes using linear codes ([14, 15]). Determining the set of minimal codewords is hard for general linear codes, although this has been studied for some classes of specific linear codes. This led to work on how to find codes where all codewords are minimal, in order to facilitate the choice of access structures. The problem of finding a code satisfying this condition, called a *minimal linear code* has first been envisioned in [11] and later studied in [6, 20, 21].

In [6], the motivation for finding minimal linear codes is no longer secret sharing but in a new proposal for secure two-party computation, where it is required that minimal linear codes be used to ensure privacy.

Minimal codes are close to the notions of intersecting and separating codes [7, 8, 16], hashing and parent-identifying codes [1, 10]. Such codes have been suggested for applications to oblivious transfer [5], secret sharing [2, 3, 11, 20] broadcast encryption or digital fingerprinting [19].

We mainly consider here the less studied and more involved non-binary case, where the notion of minimal codes is more restrictive than that of separating codes. This extension is meaningful, since secret-sharing and secure two-party computations both require a large alphabet.

2010 *Mathematics Subject Classification:* 94B25, 94B27, 05D40.
Key words and phrases: Linear codes, minimal codes, quasi-minimal codes.

We continue in Section 2 the study of [9] on bounds and criteria for minimal linear codes and exhibit families of minimal codes with better rates (asymptotically non-zero). In Section 3, we relax the notion of minimal codes and introduce *quasi-minimal* linear codes. Quasi-minimal linear codes are codes where two non-zero codewords have the same support if and only if they are linearly dependent. This slight relaxation enables to exhibit families with improved non-zero asymptotic rates.

Finally, we consider yet another generalization to t-minimal and t-quasi-minimal codes, where we impose that these conditions of non-inclusion or non-equality of the supports should be guaranteed by at least t of the coordinates.

2. Minimal codes: bounds and constructions

2.1. Notation and preliminaries. We denote by $|F|$ the cardinality of a set F. Let $q = p^h$, where p is a prime number and $h \in \mathbb{N}*$. An $[n, k, d, d_{max}]_q$ code is a vector subspace of $\mathbb{F}_q^n$ of dimension k . The last two parameters refer to the minimal (resp. maximal) Hamming distance between two codewords of $\mathcal{C}$, or, equivalently, the minimal (resp. maximal) Hamming weight of a codeword of $\mathcal{C}$; they will be omitted when irrelevant. Normalized parameters will be denoted by $R = k/n, \delta = d/n, \delta_{max} = d_{max}/n$.

The *support* of a codeword $c \in \mathcal{C}$ is $supp(c) = \{i \in \{1, \ldots, n\} | c_i \neq 0\}$. The *Hamming weight* of a codeword $c \in \mathcal{C}$ denoted by $wt(c)$ is the cardinality of its support : $wt(c) = |supp(c)|$. A codeword c *covers* a codeword c' if $supp(c') \subset supp(c)$.

A code is *intersecting* if the intersection of the supports of two nonzero codewords is not empty.

Definition 1 (Minimal codeword)**.** A codeword c is *minimal* if it only covers $\mathbb{F}_q \cdot c$, *i. e.* if $\forall c' \in \mathcal{C}, (supp(c') \subset supp(c)) \implies (c, c')$ linearly dependent.

Definition 2 (Minimal linear code, [11])**.** A linear code $\mathcal{C}$ is *minimal* if every (non-zero) codeword $c \in \mathcal{C}$ is minimal.

Note that this definition of minimality differs from the one in [14], where the leftmost non-zero component of a minimal codeword is restricted to be 1. Both definitions seem to co-exist; the one we adopt here is closer to the set-theoretic interpretation.

For a complete treatment and general references in coding theory, we refer to the book of MacWilliams and Sloane [13].

2.2. Bounds. Two non-constructive bounds on the rates of minimal codes are exhibited in [6]. We recall them without proofs.

Theorem 3 (Maximal Bound, [6])**.** *Let $\mathcal{C}$ a minimal linear $[n, k, d]$ q-ary code, then $R \leq \log_q(2)$.*

Theorem 4 (Minimal Bound, [6])**.** *For any R, $0 \leq R = k/n \leq \frac{1}{2}\log_q(\frac{q^2}{q^2-q+1})$, there exists an infinite sequence of $[n, k]$ minimal linear codes.*

2.3. A sufficient condition. If the weights of a linear code are close enough to each other, then each (non-zero) codeword of the code is a minimal vector as described by the following statement.

Proposition 5 ([2]). *Let $\mathcal{C}$ be an $[n,k,d,d_{max}]$ code. If $\frac{d}{d_{max}} > \frac{q-1}{q}$ then $\mathcal{C}$ is minimal.*

Remark 6. Note that the stronger sufficient condition $\frac{d}{n} > \frac{q-1}{q}$ fails to provide asymptotically good codes; indeed, by the Plotkin bound ([13], for any code, not necessarily linear, of length n, size M and distance d, if $d > (q-1)n/q$, then $M \leq d/(d-(1-q^{-1}))$.

On the other hand, for $\delta < 1 - q^{-1}$, the classical Varshamov-Gilbert bound [12] guarantees the existence of asymptotic families of codes with non-zero rate $R(\delta, q)$.

Remark 7. The previous condition is only sufficient, as proved in [9]: start with the celebrated tetracode $T[4,2,3,3]_3$. Consider its iterated tensor (Kronecker) powers (see later for a definition); one gets successively $T^2[16,4,9,12]$ and $T^4[256,16,81,\geq 144]$. This code does not satisfy the condition but is nevertheless minimal.

Remark 8. On the other hand, this condition is tight, as shown by the non-minimal Reed-Solomon $RS[q,2,q-1,q]_q$ code generated when $q=p$ is prime by the two codewords $(0,1,2...,p-1)$ and $(1,1,...,1)$ of weight $p-1$ and p respectively.

2.4. INFINITE CONSTRUCTIONS. The general idea is to concatenate a q-ary "seed" or inner code (e.g. a simplex) with an infinite family of algebraic-geometric (AG) codes (the outer codes) [22], in such a way as to obtain a high enough minimum distance and conclude by Proposition 5.

In practice, we can take the seed to be the simplex code $\mathcal{S}_{q,r}[n=(q^r-1)/(q-1), k=r, d=d_{max}=q^{r-1}]_q$ (with $\delta > (q-1)/q$), set $r=2m$ and concatenate with $AG[N, K=NR, D=N\Delta, D_{max}=N\Delta_{max}]_{q^{2m}}$. These codes exist lying almost on the Singleton bound, namely satisfying $R+\Delta = 1-(q^m-1)^{-1} > (q-1)/q$.

This concatenation results in the family $C[nN, kK, dD]_q$ with maximum distance at most $d_{max}N$. If $dD/d_{max}N = \Delta > (q-1)/q$, this family is minimal by Proposition 5.

It is not hard to check that, for example, choosing q large and α small enough, $m \geq 2, \Delta = (q-1)/q + \alpha, R = 1/q - 1/(q^m-1) - \alpha > 0$, this is the case.

To summarize, we construct infinite families of codes with $R = 2m(1/q - 1/(q^m-1) - \alpha)(q-1)/(q^{2m}-1) \approx 2m/q^{2m}$ satisfying $\delta/\delta_{max} > (q-1)/q$, thus minimal. Note that, by the Plotkin bound, they necessarily satisfy $\delta < (q-1)/q$, so the fact that $\delta_{max} < 1$ is crucial.

3. QUASI-MINIMAL CODES

We now relax the notion of minimal codes to that of *quasi-minimal* codes. In words, minimality prevents a codeword from having its support included in the support of a linearly independent codeword, whereas quasi-minimality only prevents two linearly independent codewords from having the same support.

3.1. DEFINITIONS AND PROPERTIES.

Definition 9 (Quasi-minimal codeword)**.** A codeword c is *quasi-minimal* if $\forall c' \in \mathcal{C}, (supp(c') = supp(c)) \implies (c, c')$ linearly dependent.

Definition 10 (Quasi-minimal linear code)**.** A linear code $\mathcal{C}$ is *quasi-minimal* if every (non-zero) codeword $c \in \mathcal{C}$ is quasi-minimal.

Quasi-minimality is clearly weaker than minimality. For instance, every binary code is quasi-minimal.

3.2. A CONSTRUCTION. We now recall a construction from [9] based on the Kronecker (tensor) product of codes, which yields infinite families of quasi-minimal codes with relatively slowly decreasing rates. The proof we provide here is slightly different and paves the way for a generalisation (see Proposition 26).

Proposition 11. *The Kronecker product $\mathcal{C}_1 \otimes \mathcal{C}_2$ of a quasi-minimal $[n_1, k_1, d_1, (d_{max})_1]_q$ code $\mathcal{C}_1$ and of a quasi-minimal $[n_2, k_2, d_2, (d_{max})_2]_q$ code $\mathcal{C}_2$ is a quasi-minimal $[n_1 \times n_2, k_1 \times k_2, d_1 \times d_2, d_{max} \geq (d_{max})_1 \times (d_{max})_2]_q$ code.*

The parameters are easy to check, so in the following proof we focus on quasi-minimality. Also we can suppose $q > 2$, otherwise there is nothing to prove.

Proof. We view codewords of $C_1 \otimes C_2$ as matrices with rows in C_2 and columns in C_1. So given two codewords $m, m' \in C_1 \otimes C_2$, we let $r^i, r'^i \in C_2$ be their i-th row and $c^j, c'^j \in C_1$ their j-th column, respectively.

Now suppose $supp(m) = supp(m')$. Then for each i, j we have $supp(r^i) = supp(r'^i)$ and $supp(c^j) = supp(c'^j)$. By quasi-minimality, this means $r'^i = \lambda_i r^i$ and $c^j = \mu_j c'^j$ for some $\lambda_i, \mu_j \in \mathbb{F}_q^\times$.

To conclude it suffices to show all λ_i with $r^i \neq 0$ are equal. So suppose $r^{i_1}, r^{i_2} \neq 0$. Since $q > 2$, C_2 is intersecting (see Proposition 19 below), so we can choose $j \in supp(r^{i_1}) \cap supp(r^{i_2})$. Looking at the (i_1, j) and (i_2, j) entries, we find $\lambda_{i_1} = \mu_j = \lambda_{i_2}$, as claimed. □

3.3. A SUFFICIENT CONDITION. We now state a sufficient condition from [9] for quasi-minimality, weaker than the one for minimality. This allows us to construct improved infinite classes of asymptotically good quasi-minimal codes by concatenation. We provide a generalised version of this result and its proof later (see Theorem 27).

Theorem 12. *Let C be a linear $[n, k, d, d_{max}]_q$ code; if $d/d_{max} > (q-2)/(q-1)$, then C is quasi-minimal.*

Example 13. For $q = 3$, consider the code $G[11, 5, 6, 9]_3$ obtained by shortening the extended ternary Golay code([13]). It is quasi-minimal by the previous theorem. Its (Kronecker) square is G^2, a $[121, 25, 36, \geq 81]_3$ quasi-minimal code by the previous proposition, although is does not satisfy the sufficient condition of Theorem 12.

Remark 14. Once again, the condition cannot be improved in general, as shown by the trivial code $[2, 2, 1, 2]_3$, formed by taking all ternary vectors of length 2, which is obviously not quasi-minimal yet satisfies $d/d_{max} = 1/2$.

Now, the celebrated non-constructive Varshamov-Gilbert bound implies the existence of infinite families of semi-constructive quasi-minimal codes with rate $R = 1 - h_q(\frac{q-2}{q-1}) > 0$. This is still far from the upper bound, derived analogously to the minimal case:

Theorem 15 (Maximal Bound)**.** *Let $\mathcal{C}$ be a quasi-minimal linear $[n, k, d]_q$ code, then $R \leq \log_q(2)$.*

3.4. INFINITE CONSTRUCTIONS OF QUASI-MINIMAL CODES. Again, we concatenate a q-ary inner code (e.g. a simplex) with an infinite family of algebraic-geometric (AG) codes to get a high enough minimum distance and conclude by Theorem 12.

Continue taking for seed $\mathcal{S}_{q,r}[n = (q^r - 1)/(q-1), k = r, d = d_{max} = q^{r-1}]_q$, set $r = 2m$ and concatenate with $AG[N, K = NR, D = N\Delta]_{q^{2m}}$, obtaining the

family $C[nN, kK, dD]_q$. Analogously to the minimal case, If $dD/d_{max}N = \Delta > (q-2)/(q-1)$, this family is quasi-minimal by Theorem 12.

Example 16.
- Taking $q = 4, \mathcal{S}_{4,4}[85, 4, 64]_4, \Delta \geq 2/3, R = 4/15$, results in an infinite construction of $[n, 16n/1275]$ quaternary codes.
- For $q = 3$, we can improve on the simplex code seed: take again $C[11, 5, 6, 9]_3$ as inner code and $AG[N, NR, N\Delta]_{3^5}$ with $R + \Delta = 191/208$. Choose $\Delta = 3/4, R = 35/208$; then concatenation results in an infinite construction of quasi-minimal $[n, \approx 0.076n]$ ternary codes.

Note that the last example relies on AG codes over fields of *odd* degree, which is quite uncommon. This was made possible only thanks to the very recent results from [4] concerning the number of points on curves over these fields; the interested reader will find in [17, 18] another application of these results to a quite different problem.

4. Strengthening: t-minimal and t-quasi-minimal codes

Minimal and quasi-minimal linear codes are defined by conditions of non-inclusion or non-equality of the supports of linearly independent codewords. We now strengthen these notions by requesting that these conditions of non-inclusion or non-equality be guaranteed by at least $t \geq 1$ of the coordinates.

4.1. Definition and properties.

Definition 17.
- A codeword c is *t-minimal* if:
$$\forall c' \in C, (|supp(c') \setminus supp(c)| < t) \implies c' \in \mathbb{F}_q \cdot c.$$
- A codeword c is *t-quasi-minimal* if:
$$\forall c' \in C, (|supp(c') \triangle supp(c)| < t) \implies c' \in \mathbb{F}_q^\times \cdot c.$$

Here $\triangle$ denotes symmetric difference $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Note that for $t = 1$ this definition reduces to the previous notions of minimality and quasi-minimality. It also makes sense when c is the zero codeword.

Definition 18. A linear code C is *t-minimal* (resp. *t-quasi-minimal*) if every codeword $c \in C$ is t-minimal (resp. t-quasi-minimal).

Proposition 19. *We have the following diagram of implications between properties of C:*

$$\begin{array}{ccccc} t\text{-minimal} & \Longrightarrow & \text{minimal} & \Longrightarrow & \text{intersecting} \\ \Downarrow & & \Downarrow & \swarrow_{q>2} & \\ t\text{-quasi-minimal} & \Longrightarrow & \text{quasi-minimal} & & \end{array}$$

with the last one holding only for $q > 2$.

Proof. The left square of implications is obvious. Now by contradiction suppose C is not intersecting, so there are $c, c' \in C$ with disjoint supports. Then $supp(c)$ is contained in $supp(c + c')$, so C is not minimal. Moreover if $q > 2$, choose $\lambda \in \mathbb{F}_q$, $\lambda \neq 0, 1$. Then $c + c'$ and $c + \lambda c'$ are linearly independent with the same support, so C is not quasi-minimal. □

4.2. UPPER BOUNDS. We let $A_q(n,d)$ be the maximal cardinality of a q-ary code of length n and minimum distance d, and then $a_q(n,d) = \log_q A_q(n,d)$ and $\alpha_q(\delta) = \limsup_n \frac{a_q(n,\lfloor \delta n \rfloor)}{n}$.

Lemma 20. *Let C be an $[n,k]$ code over $\mathbb{F}_q$ and let $c \in C$ be t-minimal of Hamming weight w. Then, projecting C on the complement of the support of c yields an $[n-w, k-1, t]$ code.*

Proof. Indeed, the kernel of this projection has dimension one (being spanned by c). □

Theorem 21. *Let C be an $[n,k,d,d_{\max}]$ code. Suppose C is t-minimal. Then $\dim C \leq 1 + a_q(n - d_{\max}, t)$.*

As a consequence, an asymptotic family of t-minimal codes with $k \sim Rn$, $d_{\max} \sim \delta_{\max} n$, and $t \sim \tau n$, can exist only if $R \leq \alpha_q(\tau/(1-\delta_{\max}))$.

Proof. Apply Lemma 20. □

On the other hand for t-quasi-minimality we have:

Theorem 22. *Let C be an $[n,k]$ code. Suppose C is t-quasi-minimal. Then $k \leq \log_q A_2(n,t)$.*

As a consequence, an asymptotic family of t-quasi-minimal codes with $k \sim Rn$ and $t \sim \tau n$ can exist only if $R \leq \log_q(2)\alpha_2(\tau)$.

Proof. By quasi-minimality, codewords of C are determined by their supports. And then by t-quasi-minimality, the characteristic functions of these supports form a binary code of minimum distance at least t. □

4.3. (ASYMPTOTIC) LOWER BOUNDS.

Lemma 23. *For any real $y \geq 1$ and $0 < \tau < \frac{q-1}{y+q-1}$ we have*

$$\sum_{i=0}^{\lfloor \tau n \rfloor} \binom{n}{i} (q-1)^i y^{n-i} = q^{n((1-\tau)\log_q(y) + H_q(\tau) + o(1))}$$

as $n \to \infty$, where $H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$ is the q-ary entropy function.

Proof. This is a very standard computation. Its main steps are:

- The sum has same order of magnitude as its maximal term.
- The ratio between consecutive terms is $\frac{n-i}{i+1} \times \frac{q-1}{y} > 1$ for $i < \lfloor \tau n \rfloor$ and $n \to \infty$, thanks to our condition $0 < \tau < \frac{q-1}{y+q-1}$.
- Hence the maximal term is for $i = \lfloor \tau n \rfloor$, and the given estimation follows from Stirling's formula. □

Theorem 24. *Suppose $\tau < \frac{q-1}{q^2}$ and*

$$R < 1 - \frac{1}{2}((1-\tau)\log_q(q^2 - q + 1) + H_q(\tau)).$$

Then there exists an asymptotic family of $[n,k]$ codes that are t-minimal, with $k \sim Rn$ and $t \sim \tau n$.

Proof. First we count the number N of "bad pairs", which means ordered pairs of words (a, b) with $(|supp(b)\backslash supp(a)| < t)$. So a pair is bad iff there are $i < t$ positions where $(a_i, b_i) = (0, \neq 0)$, while in the remaining $n - i$ positions $(a_i, b_i) \neq (0, \neq 0)$. Hence using Lemma 23 we find

$$N = \sum_{i=0}^{t-1} \binom{n}{i} (q-1)^i (q^2-q+1)^{n-i} = q^{n((1-\tau)\log_q(q^2-q+1)+H_q(\tau)+o(1))}.$$

Among these there are $O(q^n)$ pairs with (a, b) linearly dependent, which is negligible (indeed, the term $i = 0$ in the sum already gives $N \geq (q^2 - q + 1)^n \geq (\frac{3}{2}q)^n$).

On the other hand, the number of $[n, k]$ codes is the Gaussian binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$. A pair of linearly independent words is contained in $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ such codes. Now we have $\begin{bmatrix} n \\ k \end{bmatrix} \cdot \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}^{-1} = q^{2n(1-R+o(1))} > N$ by our hypothesis on R, or said otherwise, $\begin{bmatrix} n \\ k \end{bmatrix} > N \cdot \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$. From this we conclude that there is at least one $[n, k]$ code that contains no bad pair, which means it is t-minimal, as claimed (and in fact, as n goes to infinity, any random code will do the job with probability 1). □

Theorem 25. *Suppose* $\tau < \frac{2q-2}{q^2}$ *and*

$$R < 1 - \frac{1}{2}((1-\tau)\log_q(q^2/2 - q + 1) + H_q(\tau) + \log_q(2)).$$

Then there exists an asymptotic family of $[n, k]$ *codes that are* t*-quasi-minimal, with* $k \sim Rn$ *and* $t \sim \tau n$.

Proof. As above we count the number N of "bad pairs", which means ordered pairs of words (a, b) with $(|supp(b) \triangle supp(a)| < t)$. So a pair is bad iff there are $i < t$ positions where $(a_i, b_i) = (0, \neq 0)$ or $(\neq 0, 0)$, while in the remaining $n - i$ positions $(a_i, b_i) \neq (0, \neq 0), (\neq 0, 0)$. We find

$$\begin{aligned} N &= \sum_{i=0}^{t-1} \binom{n}{i} (2q-2)^i (q^2-2q+2)^{n-i} \\ &= 2^n \sum_{i=0}^{t-1} \binom{n}{i} (q-1)^i (q^2/2-q+1)^{n-i} \\ &= q^{n((1-\tau)\log_q(q^2/2-q+1)+H_q(\tau)+\log_q(2)+o(1))} \end{aligned}$$

and we conclude likewise. □

4.4. A CONSTRUCTION. We now extend Proposition 11 to higher (quasi) minimality.

Proposition 26. *Let* C_1 *be* t_1*-minimal (resp.* t_1*-quasi-minimal) and* C_2 *be* t_2*-minimal (resp.* t_2*-quasi-minimal). Then* $C_1 \otimes C_2$ *is* $t_1 t_2$*-minimal (resp.* $t_1 t_2$*-quasi-minimal).*

Proof. We view codewords of $C_1 \otimes C_2$ as matrices with rows in C_2 and columns in C_1. So given two codewords $m, m' \in C_1 \otimes C_2$, we let $r^i, r'^i \in C_2$ be their i-th row and $c^j, c'^j \in C_1$ their j-th column, respectively.

First we deal with minimality. Suppose

$$|supp(m') \setminus supp(m)| < t_1 t_2.$$

Set

$$I = \{i;\ |supp(r'^i) \setminus supp(r^i)| \geq t_2\},$$
$$J = \{j;\ |supp(c'^j) \setminus supp(c^j)| \geq t_1\}.$$

Then necessarily we have $|I| < t_1$ and $|J| < t_2$.

Now since C_2 is t_2-minimal, for each $i \notin I$, there is $\lambda_i \in \mathbb{F}_q$ such that $r'^i = \lambda_i r^i$. This implies that for each j, we have $supp(c'^j) \setminus supp(c^j) \subset I$, so $|supp(c'^j) \setminus supp(c^j)| \leq |I| < t_1$, which means $J = \emptyset$. By symmetry we also get $I = \emptyset$.

To conclude it suffices to show all λ_i with $r^i \neq 0$ are equal. So suppose $r^{i_1}, r^{i_2} \neq 0$. By Proposition 19, C_2 is intersecting, so we can choose $j \in supp(r^{i_1}) \cap supp(r^{i_2})$. Then, since $J = \emptyset$ and C_1 is t_1-minimal, there is $\mu_j \in \mathbb{F}_q$ such that $c'^j = \mu_j c^j$. Looking at the (i_1, j) and (i_2, j) entries, this gives $\lambda_{i_1} = \mu_j = \lambda_{i_2}$, as claimed.

Now we deal with quasi-minimality. For $q = 2$ the result is already known, since t-quasi-minimality just means minimum distance at least t. So we can suppose $q > 2$. We then proceed exactly as above, with symmetric difference $\triangle$ replacing ordinary set difference $\setminus$, and with the λ_i in $\mathbb{F}_q^\times$ instead of $\mathbb{F}_q$. In the last step we will need C_2 to be intersecting, which is true for $q > 2$ by Proposition 19 again. □

4.5. A SUFFICIENT CONDITION. We prove here an extension of Theorem 12 to t-quasi-minimality.

Theorem 27. *Let C be a linear $[n, k, d, d_{max}]_q$ code. If $(q-1)d > (q-2)d_{max} + q(t-1)/2$, then C is t-quasi-minimal.*

Proof. Let C be a linear $[n, k, d]_q$ code and let c, c' be two linearly independent codewords of C such that $|supp(c') \triangle supp(c)| < t$. Let α be a primitive element of $\mathbb{F}_q$. Then, w.l.o.g., after a suitable permutation of coordinates, one can write c and c' by blocks, in the following way (where η and θ denote blocks of nonzero elements with total length $|\eta| + |\theta| \leq t$):

$$c = \beta_0 || \dots || \beta_{q-2} || \eta || 0 || 0 ||,$$
$$c' = \alpha^0 \beta_0 || \dots || \alpha^{q-2} \beta_{q-2} || 0 || \theta || 0.$$

Let A_i be the size of the (possibly empty) block β_i. Then $wt(\alpha^j c) = \sum_{i=0}^{q-2} A_i + |\eta|$ and $wt(c') = \sum_{i=0}^{q-2} A_i + |\theta|$. We also have, for $j = 0, \dots, q-2$, $S_j := d(\alpha^j c, c') = \sum_{i \neq j} A_i + |\eta| + |\theta| \geq d$. If we sum all these inequalities and set $S := \sum S_j$, we get

$$\begin{aligned}(q-1)d \leq S &= (q-2)\sum_{i=0}^{q-2} A_i + (q-1)(|\eta| + |\theta|) \\ &= (q-2)(wt(c) + wt(c'))/2 + q(|\eta| + |\theta|)/2 \\ &\leq (q-2)d_{max} + q(t-1)/2,\end{aligned}$$

a contradiction. Thus, c and c' cannot exist and C is t-quasi-minimal. □

Final Questions. - *Is it true that the best achievable rate of (t) (quasi)- minimal codes is a decreasing function of q? A weaker statement holds: if q divides q', then a q'- ary (t) (quasi)- minimal code yields a q-ary (t) (quasi)-minimal code with the same rate.*

- *We have studied quite a few extensions of the original notion of minimality; it is definitely an interesting future research topic to find applications for those.*

ACKNOWLEDGMENTS

We gratefully acknowledge the support of Project SecuLar ANR-12-CORD-014.

REFERENCES

[1] N. Alon, G. Cohen, M. Krivilevitch and S. Litsyn, Generalized hashing and applications, *JCT-A*, **104** (2003), 207–215.
[2] A. Ashikhmin and A. Barg, Minimal vectors in linear codes, *IEEE Trans. Inf. Theory*, **44** (1998), 2010–2017.
[3] A. Ashikhmin, A. Barg, G. Cohen and L. Huguet, Variations on minimal codewords in linear codes, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer, 1995, 96–105.
[4] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, Towers of function fields over non-prime finite fields, *Moscow Math. J.*, **15** (2015), 1–29.
[5] G. Brassard, C. Crépeau and M. Santha, Oblivious transfers and intersecting codes, *IEEE Trans. Inf. Theory*, **42** (1996), 1769–1780.
[6] H. Chabanne, G. Cohen and A. Patey, Towards secure two-party computation from the wire-tap channel, in *Information Security and Cryptology–ICISC 2013*, Springer, 2013, 34–46.
[7] G. Cohen, S. Encheva, S. Litsyn and H.-G. Schaathun, Intersecting codes and separating codes, *Discrete Appl. Math.*, **128** (2003), 75–83.
[8] G. Cohen and A. Lempel, Linear intersecting codes, *Discrete Math.*, **56** (1985), 35–43.
[9] G. Cohen, S. Mesnager and A. Patey, On minimal and quasi-minimal linear codes, in *Proc. 14th Int. Conf. Crypt. Coding*, Springer, Heidelberg, 2013, 85–98.
[10] G. Cohen and H.-G. Schaathun, Upper bounds on separating codes, *IEEE Trans. Inf. Theory*, **50** (2004), 1291–1295.
[11] C. Ding and J. Yuan, Covering and secret sharing with linear codes, in *DMTCS*, Springer, 2003, 11–25.
[12] E. N. Gilbert, A comparison of signaling alphabets, *Bell Syst. Techn. J.*, **31** (1952), 504–522.
[13] F. J. MacWilliams and N. J. Sloane, *The theory of error-correcting codes*, North Holland, Amsterdam, 1977.
[14] J. L. Massey, Minimal codewords and secret sharing, in *Proc. 6th Joint Swedish-Russian Int. Workshop Info. Theory*, 1993, 276–279.
[15] J. L. Massey, Some applications of coding theory in cryptography, in *Codes and Cyphers: Cryptography and Coding IV* (ed. P.G. Farrell), 1995, 33–47.
[16] H. Randriambololona, $(2,1)$-separating systems beyond the probabilistic bound, *Israel J. Math.*, **195** (2013), 171–186.
[17] H. Randriambololona, Asymptotically good binary linear codes with asymptotically good self-intersection spans, *IEEE Trans. Inf. Theory*, **59** (2013), 3038–3045.
[18] H. Randriambololona, On products and powers of linear codes under componentwise multiplication, in *Proc. 14th Int. Conf. Arithm. Geom. Crypt. Coding Theory (AGCT-14)*, Luminy, 2015, 3–7.
[19] H. G. Schaathun, The Boneh-Shaw fingerprinting scheme is better than we thought, *IEEE Trans. Inf. Forensics Sec.*, **1** (2006), 248–255.
[20] Y. Song and Z. Li, Secret sharing with a class of minimal linear codes, preprint, arXiv:1202.4058
[21] Y. Song, Z. Li, Y. Li and J. Li, A new multi-use multi-secret sharing scheme based on the duals of minimal linear codes, *Sec. Commun. Netw.*, **8** (2015), 202–211.
[22] M. A. Tsfasman and S. G. Vladut, *Algebraic Geometric Codes*, Kluwer, 1991.

Received December 2014; revised May 2015.

E-mail address: cohen@telecom-paristech.fr
E-mail address: smesnager@univ-paris8.fr
E-mail address: randriam@telecom-paristech.fr