On Minimal and Quasi-minimal Linear Codes

Gérard Cohen[1,4], Sihem Mesnager[2], and Alain Patey[1,3,4]

[1] Télécom ParisTech, CNRS LTCI
{gerard.cohen,alain.patey}@telecom-paristech.fr
[2] Department of Mathematics, University of Paris VIII, LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, and University of Paris XIII, Sorbonne Paris Cité
smesnager@univ-paris8.fr
[3] Morpho
alain.patey@morpho.com
[4] Identity and Security Alliance (The Morpho and Télécom ParisTech Research Center)

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 here study minimal codes, give new bounds and properties and exhibit families of minimal linear codes. We also introduce and study the notion of quasi-minimal linear codes, which is a relaxation of the notion of minimal linear codes, where two non-zero codewords have the same support if and only if they are linearly dependent.

Keywords: minimal codes, quasi-minimal codes, intersecting codes, secret sharing.

1 Introduction

A *minimal codeword* [15,16] 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. Determining the set of minimal codewords is difficult 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 [10] and later studied in [20,4].

Interestingly, in [4], 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 are used to ensure privacy.

It is pointed out in [4] that minimal codes are close to the notions of intersecting and separating codes [7,6]. Such codes have been suggested for applications to oblivious transfer [2], secret sharing [1,10,20] or digital fingerprinting [18].

M. Stam (Ed.): IMACC 2013, LNCS 8308, pp. 85–98, 2013.

In the binary case, the notions of intersecting and minimal linear codes coincide. Intersecting codes have already received a lot of attention [7,19,8,2,11]. For instance, [7] gives definitions, some generic constructions and non-constructive bounds on rates; [19] gives explicit constructions for small dimensions and summarizes bounds on minimum distance; [8] gives an explicit constructive sequence of intersecting codes with high rate, and so on. We will not here focus on the binary case, but on the q-ary case, where the notion of minimal codes is more restrictive than the notion of separating codes. Secret-sharing and secure two-party computations both crucially hinge on a large alphabet; thus, one cannot rely on the well-understood binary case only.

We thus pursue in Section 2 the study of [4] on bounds and criteria for minimal linear codes and exhibit families of minimal codes with better rates (but still asymptotically zero). We also exhibit in Section 3 new constructions of minimal codes using trace functions, following the works of [10,20]. Finally, in Section 4, 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 non-zero asymptotic rates.

2 Minimal Codes – Bounds and Constructions

2.1 Definitions – Notations

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 $[n, k, d]_q$ code is a vector subspace of $\mathbb{F}_q^n$ of dimension k with minimum Hamming distance d; d_{max} is the maximal distance between two codewords of $\mathcal{C}$. Normalized parameters will be denoted by $R = k/n, \delta = d/n, \delta_{max} = d_{max}/n$; R is called the *rate* of $\mathcal{C}$.

The *support* of a codeword $c \in \mathcal{C}$ is the set $supp(c) = \{i \in \{1, \ldots, n\} | c_i \neq 0\}$. 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 $supp(c') \subset supp(c)$.

Definition 1 (Minimal codeword). *[15] 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). *[10] A linear code $\mathcal{C}$ is minimal if every non-zero codeword $c \in \mathcal{C}$ is minimal.*

A code $\mathcal{C}$ is *intersecting* if $\forall c \neq 0, c' \neq 0 \in \mathcal{C}, supp(c) \cap supp(c') \neq \emptyset$. A code $\mathcal{C}$ is *t-intersecting* if $\forall c \neq 0, c' \neq 0 \in \mathcal{C}, |supp(c) \cap supp(c')| \geq t$

For a complete treatment of coding theory, we refer to the book of MacWilliams and Sloane [14].

2.2 Generic Bounds

Two non-constructive bounds on the rates of minimal codes are exhibited in [4]. We recall them with their proofs. Notice that these constructions are more demanding as q grows.

Theorem 1 (Maximal Bound). *[4] Let $\mathcal{C}$ a minimal linear $[n,k,d]$ q-ary code, then, asymptotically, $R \leq \log_q(2)$.*

Proof. This bound is even true for non-linear minimal codes. Let us consider the family F of supports of the vectors of $\mathcal{C}$. By definition of minimal codes, this is a Sperner family. It is known that $|F| \leq \binom{n}{n/2}$. Thus, $|\mathcal{C}| = q^k \leq 1 + (q-1)\binom{n}{n/2}$ and $R = k/n \leq \log_q(2) + o(1)$.

Theorem 2 (Minimal Bound). *[4]*

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.

Proof. The proof is similar to the one of [7] in the binary case. Let us fix n and k. For $a \in \mathbb{F}_q^n$, such that $|supp(a)| = i$, there are $q^i - q$ linearly independent vectors b such that $supp(b) \subset supp(a)$. The pair (a,b) belongs to $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ linear $[n,k]$ codes, where $\begin{bmatrix} x \\ k \end{bmatrix}$ denotes the q-ary Gaussian binomial coefficient.

There are less than $\sum_{i=0}^{n} \binom{n}{i}(q-1)^i(q^i-q) = (1+(q-1)q)^n - q^{n+1} \leq (q^2-q+1)^n$ such ordered "bad" (a,b) pairs. At least $\begin{bmatrix} n \\ k \end{bmatrix} - \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}(q^2-q+1)^n$ linear $[n,k]$ codes thus contain no "bad" pairs, *i. e.* are minimal. For $k/n \leq \frac{1}{2}\log_q(\frac{q^2}{q^2-q+1})$, this quantity is positive.

2.3 Minimal Codes and Intersecting Codes

Proposition 1. *A minimal linear code $\mathcal{C}$ is intersecting.*

Proof. Let c, c' be two codewords such that $supp(c) \cap supp(c') = \emptyset$. We have $supp(c) \subset supp(c+c')$ and $supp(c') \subset supp(c+c')$. Thus, c and $c+c'$ are linearly dependent, c' and $c+c'$ are linearly dependent; hence c and c' are linearly dependent. Since $supp(c) \cap supp(c') = \emptyset$, at least one of c, c' is equal to zero, thus $\mathcal{C}$ is intersecting. □

The converse is true in the binary case (only).

Proposition 2. *A binary intersecting linear code $\mathcal{C}$ is minimal.*

Proof. Let C be a binary linear code. Let us assume that there exist two nonzero codewords $c \neq c'$ with $supp(c) \subset supp(c')$. The inclusion is strict since two different binary codewords cannot share the same support. the support of $c+c'$ does not intersect with the support of c. Hence, a non-minimal code is not intersecting. □

The condition of minimality is more demanding than that of intersection, and the more so when q increases. This fact is captured by the next result (which also proves that the only case where the converse of Proposition 1 is true is the binary case).

Proposition 3. *A minimal $[n,k,d]_q$ code is $(q-1)$-intersecting, if $k \geq 2$.*

Proof. Let c, c' be two linearly independent codewords. One can write by blocks, w.l.o.g., $c = 0||X||0||Z$ and $c' = 0||0||Y||Z'$, where all X, Y, Z, Z' do not contain any zeros, $|X| \geq 1$, $|Y| \geq 1$ and $|Z| = |Z'| \geq 1$ (minimality). Let $\lambda \in \mathbb{F}_q^*$, $c + \lambda c' = 0||X||\lambda Y||Z + \lambda Z'$ is independent of c and of c', consequently it should not cover either c or c'. Thus, there exists i_λ such that $z_{i_\lambda} + \lambda z'_{i_\lambda} = 0$. This must be true for any $\lambda \in \mathbb{F}_q^*$. Since all coordinates of Z and Z' are non-zero, one cannot have $i_\lambda = i_\mu$, for $\lambda \neq \mu$. Consequently $|supp(c) \cap supp(c')| \geq |\mathbb{F}_q| = q-1$. In particular, the minimum weight d of a nonzero codeword is at least $(q-1)$ and two linearly dependent nonzero codewords also intersect in at least $q-1$ positions. Thus $\mathcal{C}$ is $(q-1)$-intersecting. □

Example 1 (Simplex Code). The shortest minimal codes of dimension 2 have length $q+1$.

For instance, consider the simplex code $\mathcal{S}_{q,k}[(q^k-1)/(q-1), k, q^{k-1}]_q$, where the generator matrix's columns are a complete set of pairwise linearly independent vectors.

For $k = 2$, it is a $\mathcal{S}_{q,2}[q+1, 2, q]$ code with generator matrix $\begin{pmatrix} 1 & 0 & 1 & \dots & 1 \\ 0 & 1 & \alpha_1 & \dots & \alpha_{q-1} \end{pmatrix}$, where $\alpha_1, \dots, \alpha_{q-1}$ are all the nonzero elements of $\mathbb{F}_q$.

Corollary 1. *Let $\mathcal{C}$ be a minimal $[n,k,d]_q$ code, then*

$$d \geq k + q - 2$$

Proof. The projection on a codeword with minimal weight gives a $[d, k, d' \geq (q-1)]$ code (see the proof of Proposition 3). The Singleton bound now implies $d \geq k + d' - 1$, thus $d \geq k + q - 2$. □

Proposition 4. *Let $\mathcal{C}$ be a minimal $[n,k,d]_q$ code with maximal distance d_{max}. Then*

$$d_{max} \leq n - k + 1$$

.

Proof. Consider a codeword c_{max} of weight d_{max} and the projection of $\mathcal{C}$ on its zero coordinates, *i. e.* on $\{1, \dots, n\} \setminus supp(c_{max})$. It is a linear operation, whose kernel has dimension 1 (since c_{max} is minimal), so its rank is $k-1$ and $k - 1 \leq n - d_{max}$. □

Notice that the bounds given by the three previous results are all tight: to see this, consider the code $\mathcal{S}_{q,2}[q+1, 2, q]$ of Example 1.

2.4 Constructions

We now give a construction based on the Kronecker product of codes. which yields infinite families of minimal codes with relatively slowly decreasing rates.

Proposition 5. *The product $\mathcal{C}_1 \otimes \mathcal{C}_2$ of a minimal $[n_1, k_1, d_1]_q$ code $\mathcal{C}_1$ and of a minimal $[n_2, k_2, d_2]_q$ code $\mathcal{C}_2$ is a minimal $[n_1 \times n_2, k_1 \times k_2, d_1 \times d_2]_q$ code.*

Proof. Let $c \neq 0, c'$ be two codewords of $\mathcal{C}_1 \otimes \mathcal{C}_2$. They can both be written as $n_1 \times n_2$ matrices where rows are codewords of $\mathcal{C}_1$ and columns are codewords of $\mathcal{C}_2$. Let us assume that c covers c'. For $i = 1, \ldots, n_1$, $j = 1, \ldots, n_2$ let c_i^1 (resp. $c_i^{'1}$) be the i^{th} row of c (resp. c') and c_j^2 (resp. $c_j^{'2}$) be the j^{th} column of c (resp. c'). For every i, c_i^1 covers $c_i^{'1}$, so $\exists \lambda_i$ such that $c_i^{'1} = \lambda_i c_i^1$. With the same reasoning on the columns, for every j, there exists λ_j such that $c_j^{'2} = \lambda_j c_j^2$. Then, all the λ_i's and λ_j's are equal and there exists λ such that $c' = \lambda c$, so c and c' are linearly dependent. Thus, $\mathcal{C}_1 \otimes \mathcal{C}_2$ is minimal. □

Example 2. For $q = 3, k = 2$, the associated simplex $\mathcal{S}_{3,2}$ is the celebrated $[4, 2, 3]_3$ tetracode T. T is self-dual, both a simplex and a Hamming code. Its (Kronecker) square is T^2, a $[16, 4, 9]_3$ minimal code. More generally, the square of the $[q+1, 2, q]_q$ simplex code is a $[(q+1)^2, 4, q^2]_q$ minimal code. Repeating the process, we obtain $[(q+1)^\ell, 2^\ell, q^\ell]_q$ minimal codes, with rate $R := k/n = (2/(q+1))^\ell$.

There exists a sufficient condition on weights for a given linear code to be minimal. More precisely, if the weights of a linear code are close enough to each other, then each nonzero codeword of the code is a minimal vector as described by the following statement.

Proposition 6. *[10] Let $\mathcal{C}$ be an $[n, k, d]$ code. Let d and d_{max} be the minimum and maximum nonzero weights respectively. If $\frac{d}{d_{max}} > \frac{q-1}{q}$ then $\mathcal{C}$ is minimal.*

Remark 1. Note that the previous condition is only necessary. Indeed, the square of the tetracode is $T^2[16, 4, d = 9, d_{max} = 12]$. To see this, take as a basis for T $c^1 = 1011$, $c^2 = 0112$, giving

$$G = H = \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,2 \end{pmatrix}$$

Then $c^1, c^2, c^3 = c^1 + c^2, c^4 = c^1 + 2c^2$ is a codeword A of T^2 of weight 12:

$$\begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,2 \\ 1\,1\,2\,0 \\ 1\,2\,0\,2 \end{pmatrix}$$

Consider now $T^4[256, 16, 81]$, the square of T^2. It is easy to check that $A \otimes A \in T^2 \otimes T^2 = T^4$ has weight 144:

$$\begin{pmatrix} A & 0 & A & A \\ 0 & A & A & 2A \\ A & A & 2A & 0 \\ A & 2A & 0 & 2A \end{pmatrix}$$

Thus $d_{max}(T^4) \geq 144$ and for this minimal code, $d/d_{max} \leq 81/144 < (q-1)/q = 2/3$.

Remark 2. Note that the easier to check sufficient condition $\frac{d}{n} > \frac{q-1}{q}$ is too strong to get asymptotically good codes; indeed, by the Plotkin bound ([14], for any code, not necessarily linear, of length n, size M and distance d, if $d > (q-1)n/q$, then $M \leq d/(d-(1-q^{-1}))$.

Plotkin bound is tight, achieved with equality by simplex codes $\mathcal{S}_{q,k}[(q^k - 1)/(q-1), k, q^{k-1}]$.

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 $R(\delta, q)$. We shall come back to that later.

Example 3. The sufficient condition exposed in Proposition 6 enables to prove the minimality of several known codes. Many examples come from the codes with a limited number of weights. For instance, in [22], one can find 3-weight codes with parameters $[26, 6, 15]_3$ or $[124, 6, 90]_5$ that satisfy the sufficient condition and that have better rates than simplex codes (respectively $\mathcal{S}_{3,4}$ and $\mathcal{S}_{5,4}$).

Similarly, the $[39, 4, 28]_5$ 4-weight code exposed in [9] also meets the condition and beats the $\mathcal{S}_{5,4}$ simplex code.

3 Constructions of Minimal Linear Codes via Trace Functions

Let p be a prime, m be a positive integer and h be a positive integer, divisor of m. Set $m = hr.$ and $q = p^h$.

Definition 3 (Trace function over $\mathbb{F}_{q^r}$).
The trace function $Tr_{q^r/q} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is defined as:

$$Tr_{q^r/q}(x) := \sum_{i=0}^{r-1} x^{q^i} = x + x^q + x^{q^2} + \cdots + x^{q^{r-1}}$$

The trace function from $\mathbb{F}_{q^r}$ to its prime subfield is called the absolute trace function.

Recall that the trace function $Tr_{q^r/q}$ is $\mathbb{F}_q$-linear and satisfies the transitivity property in a chain of extension fields ($m = hr$): $Tr_{p^m/p}(x) = Tr_{p^h/p}(Tr_{p^m/p^h}(x))$ for all $x \in \mathbb{F}_{q^r}$.

Given a Boolean function f defined on $\mathbb{F}_{2^n}$ (that is, a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$), the Walsh transform of f is the discrete Fourier transform of the sign function of f that is, $\chi(f) := (-1)^f$ where χ is the canonical additive character. The Walsh transform of f denoted by $\widehat{\chi_f}$ is defined as:

$$\widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+x\cdot a}, \forall a \in \mathbb{F}_{2^n}$$

where "$\cdot$" denotes a scalar product in $\mathbb{F}_{2^n}$. The mapping $(x, y) \mapsto Tr_{2^n/2}(xy)$ defines an inner (scalar) product on $\mathbb{F}_{2^n}$. Finally, a Boolean function f on $\mathbb{F}_{2^n}$ (n even) is bent if and only if its Walsh transform satisfies $\widehat{\chi_f}(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$. The dual $\tilde{f}$ of a bent function f is defined by the relation $\widehat{\chi_f}(\omega) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\omega)}$, $\forall \omega \in \mathbb{F}_{2^n}$.

3.1 A Construction of a Class of q-ary Linear Minimal Codes

For any $\alpha, \beta \in \mathbb{F}_{p^m}$, define a q-ary function $f_{\alpha,\beta}$ as:

$$\begin{aligned} f_{\alpha,\beta} : \mathbb{F}_{q^r} &\longrightarrow \mathbb{F}_q \\ x &\longmapsto f_{\alpha,\beta}(x) := Tr_{q^r/q}(\alpha\Psi(x) + \beta x) \end{aligned}$$

where Ψ is a mapping from $\mathbb{F}_{q^r}$ to $\mathbb{F}_{q^r}$ such that $\Psi(0) = 0$. We now define a linear code $\mathcal{C}_\Psi$ over $\mathbb{F}_q$ as :

$$\mathcal{C}_\Psi := \{\bar{c}_{\alpha,\beta} = (f_{\alpha,\beta}(\zeta_1), f_{\alpha,\beta}(\zeta_2), \cdots, f_{\alpha,\beta}(\zeta_{q^r-1})), \alpha, \beta \in \mathbb{F}_{q^r}\}$$

where $\zeta_1, \cdots, \zeta_{q^r-1}$ denote the nonzero elements of $\mathbb{F}_{q^r}$.

Proposition 7. *The linear code $\mathcal{C}_\Psi$ is of length $q^r - 1$ and dimension k with $k = \frac{2m}{h} = 2r$ if the mapping Ψ has no linear components, and $k < 2r$ otherwise.*

Proof. It is clear that $\mathcal{C}_\Psi$ is of length $q^r - 1$. Now, compute the cardinality of $\mathcal{C}_\Psi$. Let $\bar{c}_{\alpha,\beta}$ be a codeword of $\mathcal{C}_\Psi$. We have

$$\begin{aligned} \bar{c}_{\alpha,\beta} = 0 &\iff Tr_{q^r/q}(\alpha\Psi(\zeta_i) - \beta\zeta_i) = 0, \forall i \in \{1, \cdots, q^r - 1\} \\ &\iff Tr_{q^r/q}(\alpha\Psi(x) - \beta x) = 0, \forall x \in \mathbb{F}_{q^r}^\star \\ &\Rightarrow Tr_{q^r/p}(\alpha\Psi(x) - \beta x) = 0, \forall x \in \mathbb{F}_{q^r}^\star \\ &\Rightarrow Tr_{q^r/p}(\alpha\Psi(x) - \beta x) = 0, \forall x \in \mathbb{F}_{q^r} \\ &\Rightarrow Tr_{q^r/p}(\alpha\Psi(x)) = Tr_{q^r/p}(\beta x), \forall x \in \mathbb{F}_{q^r} \end{aligned}$$

Hence, $\bar{c}_{\alpha,\beta} = 0$ implies that the mapping from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$, that is, a component of Ψ associated to $\alpha \neq 0$, is linear (or null) and coincides with $x \mapsto Tr_{q^r/p}(\beta x)$. Therefore, it suffices that no component function of Ψ is identically equal to 0 or linear to ensure that the only null codeword appears only one time at $\alpha = \beta = 0$. Furthermore, this implies that all the codewords $\bar{c}_{\alpha,\beta}$ are pairwise distinct. In this case, the size of the code is q^{2r} and the dimension of the code is thus $2r$. □

Assume p is an odd prime. Choose Ψ a perfect nonlinear mapping, that is, Ψ is such that $max_{a \in \mathbb{F}_{q^r}^\star} min_{b \in \mathbb{F}_q} |D_a\Psi^{-1}(b)| = \frac{q^r-1}{q^r}$ where $D_a\Psi(x)$ denotes the derivatives of Ψ defined by $D_a\Psi(x) := \Psi(x + a) + \Psi(x)$. According to [3], if $q < \frac{q^{r/2}+1}{2}$, then (using the sufficient condition given in Proposition 6) $\mathcal{C}_\Psi$ is a minimal $[q^r - 1, 2r, d > \frac{q-1}{q}(q^r - q^{r/2})]$-code.

3.2 A Construction of a Class of Linear Minimal 2^h-ary Codes

The previous construction of minimal codes is valid when p is an odd prime. In this subsection, we provide a construction of minimal codes in the case where

$p = 2$. To this end, let m be a positive integer and h a divisor of m. Set $r := \frac{m}{h}$. We define two sets E and R of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as follows:

$$E := \{(x, 0), x \in \mathbb{F}_{2^m}\},$$

and

$$R := \{(0, y), y \in \mathbb{F}_{2^m}\}.$$

Set

$$\Gamma := \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \setminus (E \cup R) = \{(\delta_i, \zeta_i), 1 \leq i \leq (2^m - 1)^2\}.$$

For any $a \in \mathbb{F}_{2^m}$, we define the function Φ_a as

$$\begin{aligned} \Phi_a : \quad \Gamma \quad &\longrightarrow \mathbb{F}_{2^h} \\ (x, y) &\longmapsto \Phi_a(x, y) := Tr_{2^m/2^h}(ax^{2^{m+1}-3}y^2) \end{aligned}$$

We now define a linear code $\mathcal{C}$ over $\mathbb{F}_{2^h}$ as :

$$\mathcal{C} := \{\bar{c}_a = (\Phi_a(\delta_1, \zeta_1), \cdots, \Phi_a(\delta_{(2^m-1)^2}, \zeta_{(2^m-1)^2})), a \in \mathbb{F}_{2^m}\}$$

It is clear that the code $\mathcal{C}$ is of length $(2^m - 1)^2$. The following statement provides the weight distribution of $\mathcal{C}$.

Proposition 8. *The linear code $\mathcal{C}$ is a one-weight minimal code. More precisely, every non-zero codeword has Hamming weight $2^{m-h}(2^h - 1)(2^m - 1)$.*

Proof. For $\omega \in \mathbb{F}_{2^m}^\star$, denote by $\psi_{a\omega}$ the Boolean function defined as follows:

$$\begin{aligned} \psi_{a\omega} : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} &\longrightarrow \mathbb{F}_2 \\ (x, y) &\longmapsto \psi_{a\omega}(x, y) := Tr_{2^m/2}(a\omega x^{2^{m+1}-3}y^2) \end{aligned}$$

Thanks to [17], the Walsh transform of $\psi_{a\omega}$ can be computed as well as its dual function. For every $a \neq 0$, we have:

$$\widehat{\chi\psi}_{a\omega}(z, t) = 2^m(-1)^{Tr_{2^m/2}(a\omega zt^{-2})}, \forall (z, t) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$$

This result implies that the function $\psi_{a\omega}$ is bent (since its Walsh transform takes only the values $\pm 2^m$) and that its dual equals $\widetilde{\psi_{a\omega}}$ defined by $\widetilde{\psi_{a\omega}}(z, t) = Tr_{2^m/2}(a\omega zt^{-2}), \forall (z, t) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. In particular, for $a \in \mathbb{F}_{2^m}^\star$ and $\omega \in \mathbb{F}_{2^m}^\star$, $\widehat{\chi\psi}_{a\omega}(0, 0) = 2^m$. Now, let us compute the value of the sum $\sum_{\omega \in \mathbb{F}_{2^h}} \widehat{\chi\psi}_{a\omega}(0, 0)$ over the subfield $\mathbb{F}_{2^h}$ of $\mathbb{F}_{2^m}$ in two ways. On the one hand, thanks to the the above expression of the Walsh transform, we get:

$$\begin{aligned} \sum_{\omega \in \mathbb{F}_{2^h}} \widehat{\chi\psi}_{a\omega}(0, 0) &= \widehat{\chi\psi}_0(0, 0) + \sum_{\omega \in \mathbb{F}_{2^h}^\star} \widehat{\chi\psi}_{a\omega}(0, 0) \\ &= 2^{2m} + 2^m(2^h - 1). \end{aligned}$$

On the other hand, using the transitivity rule of the trace function and the $\mathbb{F}_{2^h}$-linearity of the trace function $Tr_{2^m/2^h}$, we have:

$$\begin{aligned}
\sum_{\omega\in\mathbb{F}_{2^h}} \widehat{\chi_\psi}_{a\omega}(0,0) &= \sum_{\omega\in\mathbb{F}_{2^h}} \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\psi_{a\omega}(x,y)} \\
&= \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} \sum_{\omega\in\mathbb{F}_{2^h}} (-1)^{Tr_{2^m/2}(a\omega x^{2^{m+1}-3}y^2)} \\
&= \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} \sum_{\omega\in\mathbb{F}_{2^h}} (-1)^{Tr_{2^h/2}(Tr_{2^m/2^h}(a\omega x^{2^{m+1}-3}y^2))} \\
&= \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} \sum_{\omega\in\mathbb{F}_{2^h}} (-1)^{Tr_{2^h/2}(Tr_{2^m/2^h}(ax^{2^{m+1}-3}y^2)\omega)} \\
&= \sum_{(x,y)\in\mathbb{F}_{2^m}^2 | Tr_{2^m/2^h}(ax^{2^{m+1}-3}y^2)=0} 2^h \\
&= 2^h \#\{(x,y)\in\mathbb{F}_{2^m}^2 \mid Tr_{2^m/2^h}(ax^{2^{m+1}-3}y^2)=0\} \\
&= 2^h\Big(2^{2m} - \#\{(x,y)\in\mathbb{F}_{2^m}^2 \mid Tr_{2^m/2^h}(ax^{2^{m+1}-3}y^2)\neq 0\} \\
&= 2^h\Big(2^{2m} - \#\{(x,y)\in\mathbb{F}_{2^m}^2 \mid \Phi_a(x,y)\neq 0\}\Big) \\
&= 2^h\Big(2^{2m} - \#\{(x,y)\in\Gamma \mid \Phi_a(x,y)\neq 0\}\Big) \\
&= 2^{2m+h} - 2^h wt(\bar{c}_a).
\end{aligned}$$

Hence, we have the following equality:

$$2^{2m+h} - 2^h wt(\bar{c}_a) = 2^{2m} + 2^m(2^h-1)$$

from which we deduce the Hamming weight of any non-zero codeword of $\mathcal{C}$: $wt(\bar{c}_a) = 2^{2m} - 2^{2m-h} - 2^m + 2^{m-h} = 2^{m-h}(2^h-1)(2^m-1)$.

According to the previous result, the code $\mathcal{C}$ is of constant weight. The structure of linear codes of constant weight is well-known. In fact, it has been proved that such codes are equivalent to simplex codes.

The next theorem ([5], page 363) characterizes all the q-ary linear codes with constant weight in terms of simplex codes and therefore defines the structure of the code $\mathcal{C}$.

Theorem 3. *([5]) If all the nonzero codewords of a q-ary $[n,k]$- code have the same weight and no coordinate identically zero, then the code has a generator matrix of the form $(G_1, G_2, \cdots, G_t)$, where each G_i is a generator matrix of the k-dimensional simplex code $\mathcal{S}_{q,k}$ over $\mathbb{F}_q$.*

Therefore, we deduce that the code $\mathcal{C}$ defined explicitly above is a minimal code equivalent to a $(2^m-1)(2^h-1)$-multiple of the 2^h-ary simplex code $\mathcal{S}_{2^h,\frac{m}{h}}$.

The code $\mathcal{C}$ has a generator matrix of the form $(G_1, G_2, \cdots, G_{(2^m-1)(2^h-1)})$, where each G_i is a generator matrix of the $\frac{m}{h}$-dimensional simplex code over $\mathbb{F}_2^h$, (that is, a $\frac{m}{h} \times (\frac{2^m-1}{2^h-1})$ matrix whose columns are pairwise linearly independent).

Note that one can generalize the previous construction and prove the following result.

Proposition 9. *Let i be a positive integer co-prime with m. For any $a \in \mathbb{F}_{2^m}$, we define the function Φ_a^i as*

$$\begin{aligned} \Phi_a^i : \quad \Gamma \quad &\longrightarrow \mathbb{F}_{2^h} \\ (x, y) &\longmapsto \Phi_a^i(x, y) := Tr_{2^m/2^h}(ax^{2^{m+i}-2^{i+1}+1}y^{2^i}) \end{aligned}$$

Define $\mathcal{C}^i := \{\bar{c}_a = (\Phi_a^i(\delta_1, \zeta_1), \cdots, \Phi_a^i(\delta_{(2^m-1)^2}, \zeta_{(2^m-1)^2})), a \in \mathbb{F}_{2^m}\}$. Then, the linear code $\mathcal{C}^i$ over $\mathbb{F}_{2^h}$ is a minimal code with parameters $[(2^m-1)^2, \frac{m}{h}, 2^{m-h}(2^h-1)(2^m-1)]$.

4 Quasi-minimal Codes

As we have seen in the previous sections, we still have no construction of minimal codes with asymptotic nonzero rate. To obtain such constructions, we slightly relax the notion of minimal codes to the new notion of *quasi-minimal* codes. Minimal codes prevent a codeword to have its support included in the support of a linearly independent codeword, whereas quasi-minimal codes prevent a codeword to have the same support as a linearly independent codeword.

We will see that this new setting, although it also brings intersection properties, allows constructions with nonzero asymptotic rates.

4.1 Definitions and Properties

Definition 4 (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 5 (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 a weaker requirement than minimality. For instance, every binary code is obviously quasi-minimal. Still, these codes do enjoy intersection properties.

Theorem 4. *If C is quasi-minimal with $n \geq q-2, k \geq 2, q \geq 3$, then it is $(q-2)$-intersecting.*

Proof. Suppose C minimal and $c, c' \in C$ with support intersection of size $s \leq q-3$. W.l.o.g., one can write by blocks $c = 0||X||0||Z$ and $c' = 0||0||Y||Z'$ with $|Z| = |Z'| = s$, and where Z and Z' do not contain any zeros.

Then at most s elements $\lambda_i \in F_q^*$ can make $|supp(Z) \cap supp(Z + \lambda_i Z')| < s$. If $s \leq q-3$, there are at least two nonzero field elements left, say α and β, such that $Z+\alpha Z'$ and $Z+\beta Z'$ are independent and have the same support. Moreover $c+\alpha c'$ and $c+\beta c'$ will also share the same support and be linearly independent, which contradicts the minimality of C. Hence, $s > q-3$. □

We now prove a sufficient condition for quasi-minimality, weaker than the one for minimality. This relaxation will then allow us to construct infinite classes of asymptotically good quasi-minimal codes by concatenation.

Theorem 5 (Sufficient condition for quasi-minimality). *Let C be a linear $[n,k,d]_q$ code; if $d/n > (q-2)/(q-1)$, then C is 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 $supp(c) = supp(c')$. Let α be a primitive element of $\mathbb{F}_q$. Then, w.l.o.g., one can write c and c' by blocks, in the following way: $c = \beta_0 || \ldots || \beta_{q-2} || 0$ and $c' = \alpha^0 \beta_0 || \ldots || \alpha^{q-2} \beta_{q-2} || 0$. Let A_i be the size of the (possibly empty) block β_i. Then $wt(c) = wt(c') = \sum_{i=0}^{q-2} A_i \geq d$. We also have, for $j = 0, \ldots, q-2$, $d(\alpha^j c, c') = \sum_{i \neq j} A_i \geq d$. If we sum all these inequalities, we get $(q-2)\sum_{i=0}^{q-2} A_i \geq (q-1)d$, hence $wt(c) \geq \frac{q-1}{q-2} d$. Thus, if $n < \frac{q-1}{q-2} d$, $wt(c) > n$, which is impossible, so c and c' cannot exist and C is quasi-minimal. □

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

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

Proof. This bound is even true for non-linear quasi-minimal codes. Consider the family F of the supports of the vectors of $\mathcal{C}$. Clearly, $|F| \leq 2^n$. Thus, $|\mathcal{C}| = q^k \leq 1 + (q-1)2^n$ and $R = k/n \leq \log_q(2) + o(1)$.

Table 1. Estimations of the rates of semi-constructive codes

q	2	3	4	5	7
Rate of the semi-constructive code	1	0.053	0.013	0.0046	0.0011
Upper bound	1	0.63	0.5	0.43	0.36

4.2 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) [21], in such a way as to obtain a high enough minimum distance and conclude by Theorem 5.

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

This concatenation results in the family $C[nN, kK, dD]_q$. If $dD/nN = \delta\Delta > (q - 2)/(q - 1)$, this family is quasi-minimal by Theorem 5.

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

Example 4 (Small examples).

- Take $q = 4, \mathcal{S}_{4,4}[85, 4, 64]_4, \Delta = 9/10, R = 1/30$, resulting in an infinite construction of $[n, 2n/1275]$ quaternary codes.
- Take $q = 3$, $C[15, 4, 9]_3$ [13] as inner code and $AG[N, NR, N\Delta]_{3^4}$ with $R + \Delta = 7/8$. Choose $\Delta = 41/48, R = 1/48$; then $\Delta\delta = 41/80$ and by Theorem 5 the concatenation is an infinite construction of quasi-minimal $[n, n/180, 41n/80]$ ternary codes.

Concluding Remarks. We can prove, non-constructively, the existence of infinite families of codes with $\delta_{max} := d_{max}/n < 1 - \omega$, for some fixed $0 < \omega$.

To do so, observe that any nonzero n-tuple belongs to $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ linear $[n, k]$ codes, i.e. a fraction $\approx q^{n-k}$ of their total number.

Fix $\omega, 0 < \omega < 1 - q^{-1}, w := \omega n$.

The number of q-ary n-tuples of weight at least $n - w$ is $\sum_{i=0}^{w} \binom{n}{i}(q-1)^{n-i} \approx \binom{n}{w}(q-1)^{n-w} \approx 2^{nh(\omega)}(q-1)^{n(1-\omega)}$, where $h(.)$ is the binary entropy function. As in the proof of the previous theorem, if $R := R(q, \omega = \epsilon(q)) \leq 1 - h(\omega)\log_q 2 - (1-\omega)\log_q(q-1)$, then the number of "bad" vectors is negligible and there exist codes with (in fact almost all codes have) rate R and no high-weight vector (of weight larger than $n(1 - \omega)$).

Now, take a code on the Varshamov-Gilbert bound (again, almost all codes are), with $\delta = 1 - q^{-1} - \alpha$ and rate $R(q, \alpha) > 0$, with $\alpha = \alpha(\omega)$ small enough so that $\delta/\delta_{max} > (1 - q^{-1} - \alpha)/(1 - \omega) > 1 - q^{-1}$; this code will necessarily be minimal.

To summarize, for a small enough rate $R = R(q)$, there exist infinite families of codes 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.

Open Problems. We saw that obtaining explicit constructions of minimal binary linear codes with asymptotically non zero rates can be done using known

techniques (e.g. [7,8]). We can however not use the same techniques in the q-ary case, where obtaining minimal linear codes, with asymptotically non zero rates, remains an open issue. Finding such codes might be done using quasi-minimal linear codes, it would thus be interesting to find a condition for minimality specific to quasi-minimal codes.

Acknowledgements. This work was partially done during the French FUI-12 RESILIENCE project that is funded by DGCIS.

References

1. Ashikhmin, A.E., Barg, A.: Minimal vectors in linear codes. IEEE Transactions on Information Theory 44(5), 2010–2017 (1998)
2. Brassard, G., Crépeau, C., Santha, M.: Oblivious transfers and intersecting codes. IEEE Transactions on Information Theory 42(6), 1769–1780 (1996)
3. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Transactions on Information Theory 51(6), 2089–2102 (2005)
4. Chabanne, H., Cohen, G., Patey, A.: Towards Secure Two-Party Computation from the Wire-Tap Channel. ArXiv e-prints (June 2013)
5. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering codes. North Holland (1997)
6. Cohen, G.D., Encheva, S.B., Litsyn, S., Schaathun, H.G.: Intersecting codes and separating codes. Discrete Applied Mathematics 128(1), 75–83 (2003)
7. Cohen, G.D., Lempel, A.: Linear intersecting codes. Discrete Mathematics 56(1), 35–43 (1985)
8. Cohen, G.D., Zémor, G.: Intersecting codes and independent families. IEEE Transactions on Information Theory 40(6), 1872–1881 (1994)
9. Ding, C.: A class of three-weight and four-weight codes. In: Chee, Y.M., Li, C., Ling, S., Wang, H., Xing, C. (eds.) IWCC 2009. LNCS, vol. 5557, pp. 34–42. Springer, Heidelberg (2009)
10. Ding, C., Yuan, J.: Covering and secret sharing with linear codes. In: Calude, C.S., Dinneen, M.J., Vajnovszki, V. (eds.) DMTCS 2003. LNCS, vol. 2731, pp. 11–25. Springer, Heidelberg (2003)
11. Encheva, S.B., Cohen, G.D.: Constructions of intersecting codes. IEEE Transactions on Information Theory 45(4), 1234–1237 (1999)
12. Gilbert, E.N.: A comparison of signalling alphabets. Bell System Technical Journal 31(3), 504–522 (1952)
13. van Lint, J.H., Schrijver, A.: Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. Combinatorica 1(1), 63–73 (1981)
14. MacWilliams, F.J., Sloane, N.J.: The theory of error-correcting codes. North-Holland, Amsterdam (1977)
15. Massey, J.L.: Minimal codewords and secret sharing. In: Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory, pp. 276–279 (1993)
16. Massey, J.L.: Some applications of coding theory in cryptography. In: Farrell, P.G. (ed.) Codes and Cyphers: Cryptography and Coding IV, pp. 33–47. Formara Ltd. (1995)
17. Mesnager, S.: Bent functions from spreads. Fq11 proceedings (preprint 2013)

18. Schaathun, H.G.: The Boneh-Shaw fingerprinting scheme is better than we thought. IEEE Transactions on Information Forensics and Security 1(2), 248–255 (2006)
19. Sloane, N.: Covering arrays and intersecting codes. Journal of Combinatorics Designs 1, 51–63 (1993)
20. Song, Y., Li, Z.: Secret sharing with a class of minimal linear codes. CoRR abs/1202.4058 (2012)
21. Tsfasman, M.A., Vladut, S.G.: Algebraic Geometric Codes. Kluwer (1991)
22. Zhou, Z., Ding, C.: A class of three-weight cyclic codes. CoRR abs/1302.0569 (2013)