21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

On Minimal and Almost-Minimal Linear Codes

Gérard Cohen[1] and Sihem Mesnager[2*]
†

Abstract

Minimal linear codes are 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 and secure two-party computations. We pursue here the study of minimal codes and construct infinite families with asymptotically non-zero rates. We also introduce a relaxation to almost minimal codes, where a fraction of codewords is allowed to violate the minimality constraint. Finally, we construct new minimal codes based on hyperovals.

Keywords: Minimal codes, Trace codes, Secret sharing.

1. Introduction

A *minimal codeword* [1, 2] c of a linear code C is a codeword such that its support (set of nonzero 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. The problem of finding a code in which all nonzero codewords are minimal, called a *minimal linear code* has first been envisioned in [3] and later studied in [4, 5, 6].

In [5], the motivation for finding minimal linear codes is in a new proposal for secure two-party computation.

Minimal codes are close to intersecting and separating codes [7], [8], [5]. Such codes have been suggested for applications to oblivious transfer [9], secret sharing [10] ,[3],[4] or digital fingerprinting [11].

We will focus here on the q-ary case, since secret-sharing and secure two-party computations both demand a large alphabet.

We pursue in Section 2 the study of [5, 6] on bounds for minimal linear codes and construct families of minimal codes with better rates (asymptotically nonzero). We relax the notion of minimality to *almost-minimality*, thus exhibiting families with improved asymptotic rates. We also describe in Section 3 new minimal codes using trace functions and hyperovals, following the works of [3, 4, 6].

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 $[n, k, d]_q$ code is a vector subspace of $\mathbb{F}_q^n$ of dimension k with minimum Hamming distance d. Let d_{max} be the maximal distance between two codewords of $\mathcal{C}$, or, equivalently, the maximal Hamming weight of a codeword of $\mathcal{C}$. 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 $supp(c') \subset supp(c)$.

Definition 1 (Minimal codeword) *[1] A codeword c is minimal if it only covers $\mathbb{F}_q \cdot c$.*

Definition 2 (Minimal linear code) *[3] A linear code $\mathcal{C}$ is minimal if every non-zero codeword $c \in \mathcal{C}$ is minimal, i. e. if no pair (c, c') of independent codewords s is "bad" (has $supp(c') \subset supp(c)$).*

Definition 3 (Almost-minimal linear code) *A linear code $\mathcal{C}$ is said (ϵ)almost-minimal if at*

*[1]Institut Télécom, Télécom ParisTech, UMR 7539, CNRS. *cohen@telecom-paristech.fr*

†[2]LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, Sorbonne Paris Cité. *smesnager@univ-paris8.fr*

ISBN: 978-90-367-6321-9

most $q^{2\epsilon k}$ pairs of codewords are bad, for some fixed ϵ with $0 \leq \epsilon < 1/2$.

For a complete treatment of coding theory, we refer to the book of MacWilliams and Sloane [12]. We extend in the next paragraph some results of [6] to almost-minimal codes.

2.2. Bounds on almost-minimal codes

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

By definition, at most $q^{\epsilon k+1}$ codewords can share the same support. Thus, $|\mathcal{C}| = q^k \leq q^{\epsilon k+1}2^n$ and $R = k/n \leq \log_q(2)/(1-\epsilon) + o(1)$.

Theorem 5 (Minimal Bound) *For any positive $R = k/n$ such that $R \leq \frac{1}{2-2\epsilon}\log_q(\frac{q^2}{q^2-q+1}) + o(1)$, there exists an infinite sequence of $[n,k]$ almost-minimal linear codes.*

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. As long as $q^{2\epsilon k}\begin{bmatrix} n \\ k \end{bmatrix} \geq \begin{bmatrix} n-2 \\ k-2 \end{bmatrix}(q^2-q+1)^n$, there are linear $[n,k]$ codes containing no more than $q^{2\epsilon k}$ bad pairs, *i. e.* almost-minimal codes. For $k/n \leq \frac{1}{2-2\epsilon}\log_q(\frac{q^2}{q^2-q+1}) + o(1)$, this quantity is positive.

2.3. Constructions

There exists a sufficient condition on weights for a given linear code to be minimal.

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 7 *Note that the stronger sufficient condition $\frac{d}{n} > \frac{q-1}{q}$ is too demanding to get asymptotically good codes; indeed, by the Plotkin bound [12], for any code, not necessarily linear, of length n, size M and distance d, if $d > (q-1)n/q$, then $M \leq d/(d-(1-q^{-1}n))$.*

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) [13], in such a way as to obtain a high enough minimum distance and conclude by Proposition 6.

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 $R + \Delta = 1 - (q^m-1)^{-1} > (q-1)/q$.

This concatenation results in the family $C[nN, kK, dD]_q$. If $dD/nN = \delta\Delta > (q-1)/q$, minimal by Proposition 6.

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. An explicit construction of minimal linear codes via a hyperoval

Let us begin with some background related to Boolean functions theory and finite geometry.

3.1. Some additional background

Definition 8 (Trace function over $\mathbb{F}_{q^r}$) *Let q be a power of a prime number. 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.

An (n,r)-function F or (vectorial function) is a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^r}$. When $r = 1$, F is said to be a Boolean function. The component functions of F are the Boolean functions $x \mapsto Tr_1^r(vF(x)), v \neq 0$. Given a Boolean function f defined on $\mathbb{F}_{2^n}$, its Walsh transform is the discrete Fourier transform of its sign function, that is, $\chi(f) := (-1)^f$ where χ is the canonical additive character.

Definition 9 (The Walsh transform) *The Walsh transform of f denoted by $\widehat{\chi_f}$ is defined as:* $\forall a \in \mathbb{F}_{2^n}, \widehat{\chi_f}(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)}$.

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 $a \in \mathbb{F}_{2^n}$. A vectorial function is said to be bent if all its components are bent. The dual $\tilde{f}$ of a bent Boolean function f is defined by the relation $\widehat{\chi_f}(\omega) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\omega)}$, $\forall \omega \in \mathbb{F}_{2^n}$.

A hyperoval in the projective space of dimension 2 on $\mathbb{F}_{2^n}$ (denoted by $PG_2(2^n)$) can be defined as follows.

Definition 10 (Hyperoval) *A hyperoval in $PG_2(2^n)$ is a set of 2^n+2 points, no three points of them collinear (that is, lying on a line[1]).*

A certain type of polynomials on $\mathbb{F}_{2^n}$ gives rise to hyperovals in $PG_2(2^n)$:

Definition 11 (Oval polynomial) An oval polynomial *on $\mathbb{F}_{2^n}$ is a polynomial G on $\mathbb{F}_{2^n}$ such that the set $\{(1,t,G(t)), t \in \mathbb{F}_2^n\} \cup \{(0,0,1),(0,1,0)\}$ (denoted by $D(G)$) forms a hyperoval of $PG_2(2^n)$ (for short,* o-polynomial*).*

There is a close connection between hyperovals and o-polynomials since a hyperoval of $PG_2(2^n)$ can be represented by $D(G)$ where G is an o-polynomial on $\mathbb{F}_{2^n}$. In fact, there exists a necessary and sufficient condition for a mapping over $\mathbb{F}_{2^n}$ to give a hyperoval of $PG_2(2^n)$. This leads to a reformulation of the definition of an o-polynomial given as follows.

Definition 12 (Oval polynomial) *A permutation polynomial G over $\mathbb{F}_{2^n}$ is an o-polynomial if, for every $\gamma \in \mathbb{F}_{2^n}$, the function*

$$z \in \mathbb{F}_{2^n} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z} & \text{if } z \neq 0 \\ 0 & \text{if } z = 0 \end{cases}$$

is a permutation of $\mathbb{F}_{2^n}$.

3.2. A construction of a class of q-ary linear minimal codes via Segre hyperoval

Let m be a positive integer. Let us consider the set of points in $PG_2(2^m)$ defined as $D(6) := \{(1,t,t^6), t \in \mathbb{F}_{2^m}\} \cup \{(0,0,1),(0,1,0)\}$. According to Segre and Bartocci [14], for $m > 3$ odd, $D(6)$ is a hyperoval of $PG_2(2^m)$ called *Segre hyperoval*. Moreover, according to Maschietti [15], $D(6)$ is a hyperoval of $PG_2(2^m)$ if and only if, $gcd(2^m-1,6) = 1$ and the equation $x^6+x+a=0$ has either zero or two distinct solutions in $\mathbb{F}_{2^m}$ (with $m \geq 3$) for every $a \in \mathbb{F}_{2^m}$.
For $m = 3$, the equation $x^6+x+a=0$ (*) has either zero or two distinct solutions in $\mathbb{F}_{2^m}$. Indeed, if $a = 0$, then (*) admits 0 and 1 as solutions. If $a \neq 0$, then (*) is equivalent to the equation $x^7+x^2+ax=0$ (when $x \neq 0$), that is, $x^2+ax+1=0$. The latter equation has necessarily two distinct solutions which are distinct (otherwise, it would yield $a = 0$, a contradiction). Therefore, $D(6)$ is a hyperoval on $PG_2(2^m)$ with $m > 2$ odd. In the following, we construct a minimal code from a Segre hyperoval. We state the main result of this section.

Proposition 13 *Let $D(6) := \{(1,t,t^6), t \in \mathbb{F}_{2^m}\} \cup \{(0,0,1),(0,1,0)\}$ be the Segre hyperoval of $PG_2(2^m)$ with $m > 2$ odd. Define Γ as $\Gamma := \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \setminus (\{(x,0), x \in \mathbb{F}_{2^m}\} \cup \{(0,y), y \in \mathbb{F}_{2^m}\}) = \{(\delta_i,\zeta_i), 1 \leq i \leq (2^m-1)^2\}$. Let h and m be two positive integers such that h divides m. For any $a \in \mathbb{F}_{2^m}$, define the function $\Phi_a : \Gamma \longrightarrow \mathbb{F}_{2^h}$ associate to $D(6)$ by $\Phi_a(x,y) := Tr_{2^m/2^h}(ax^{3\cdot 2^{m+1}-11}y^6), \forall (x,y) \in \Gamma \times \mathbb{F}_{2^h}$. Moreover, define a linear code $\mathcal{C}$ over $\mathbb{F}_{2^h}$ as:*

$$\mathcal{C} := \{\bar{c}_a = (\Phi_a(\delta_j,\zeta_j), j \in [1,(2^m-1)^2]), a \in \mathbb{F}_{2^m}\}.$$

Then the linear code $\mathcal{C}$ is a minimal code associated to $D(6)$ with parameters $[(2^m-1)^2, \frac{m}{h}, 2^{m-h}(2^h-1)(2^m-1)]$.

Only the minimum distance and minimality assertions need checking. For every $m > 2$ odd, $D(6)$ is a hyperoval of $PG_2(2^m)$, hence $G(z) = z^6$ is an o-polynomial on $\mathbb{F}_{2^m}$. According to [16], for every $a \in \mathbb{F}_{2^m}^\star$, the $(2m,m)$-function $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \Phi_a(x,y)$ is a bent vectorial function of the form $\Phi_a(x,y) = Tr_{2^m/2^h}(axG(yx^{2^m-2}))$ with $G(z) = z^6$. Therefore, all the components of Φ_a are bent Boolean functions belonging to the class $\mathcal{H}$ introduced by Carlet and Mesnager [17]. Let $\psi_{a\omega}$ ($\omega \in \mathbb{F}_{2^m}^\star$) be a component of of Φ_a. $\psi_{a\omega}$ is of the form $\psi_{a\omega}(x,y) = Tr_{2^m/2}(a\omega x^{3\cdot 2^{m+1}-11}y^6)$. Since $\psi_{a\omega}$ is bent, its Walsh transform takes only the values $\pm 2^m$, that is, $\widehat{\chi_{\psi_{a\omega}}}(x,y) = \pm 2^m$. Now, recall that $\forall (z,t) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, $\widehat{\chi_{\psi_{a\omega}}}(z,t) = 2^m(-1)^{\tilde{\psi}_{a\omega}(z,t)}$, where $\tilde{\psi}_{a\omega}$ denotes the dual function of $\psi_{a\omega}$. According to [17], $\tilde{\psi}_{a\omega}(\alpha,\beta) = 1$ if the equation $z^6+\beta z = \alpha$ has no solution in $\mathbb{F}_{2^m}$, and 0 otherwise.

[1] We say a point $p = (x_0,\cdots,x_n)$ is on a line $L[y_0,\cdots,y_n]$ if $x_0y_0+x_1y_1+\cdots x_ny_n = 0$.

In particular, $\tilde{\psi}_{a\omega}(0,0) = 0$, that is $\widehat{\chi_{\psi_{a\omega}}}(0,0) = 2^m$. Now, on one hand, $\sum_{\omega\in\mathbb{F}_{2^h}} \widehat{\chi_{\psi}}_{a\omega}(0,0) = 2^{2m+h} - 2^h wt(\bar{c}_a)$, according to Cohen et al [6]. On the other hand, $\sum_{\omega\in\mathbb{F}_{2^h}} \widehat{\chi_{\psi}}_{a\omega}(0,0) = \widehat{\chi_{\psi}}_0(0,0) + \sum_{\omega\in\mathbb{F}^\star_{2^h}} \widehat{\chi_{\psi}}_{a\omega}(0,0)$. Hence, $\sum_{\omega\in\mathbb{F}_{2^h}} \widehat{\chi_{\psi}}_{a\omega}(0,0) = 2^{2m} + 2^m(2^h - 1)$. Collecting the two expressions of the sum $\sum_{\omega\in\mathbb{F}_{2^h}} \widehat{\chi_{\psi}}_{a\omega}(0,0)$, we deduce that the Hamming weight of any non-zero codeword of $\mathcal{C}$ equals $wt(\bar{c}_a) = 2^{2m} - 2^{2m-h} - 2^m + 2^{m-h} = 2^{m-h}(2^h - 1)(2^m - 1)$. The code $\mathcal{C}$ has constant weight equal to the claimed minimum distance, and is thus minimal, which completes the proof.

Open problem: Is it true that the best achievable rate of (almost) minimal codes is a decreasing function of q? A weaker statement holds: if q divides q', then a q'- (almost) minimal code yields a q-ary (almost) minimal code with the same rate.

Acknowledgements. We thank Alexander Barg, Alain Patey and Zachi Tamo for helpful discussions.

References

[1] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory*, 1993, pp. 276–279.

[2] ——, "Some applications of coding theory in cryptography," in *Codes and Cyphers: Cryptography and Coding IV*, P. G. Farrell, Ed. Formara Ltd, 1995, pp. 33–47.

[3] C. Ding and J. Yuan, "Covering and secret sharing with linear codes," in *DMTCS*, ser. Lecture Notes in Computer Science, C. Calude, M. J. Dinneen, and V. Vajnovszki, Eds., vol. 2731. Springer DMTCS, 2003, pp. 11–25.

[4] Y. Song and Z. Li, "Secret sharing with a class of minimal linear codes," *CoRR*, vol. abs/1202.4058, 2012.

[5] H. Chabanne, G. Cohen, and A. Patey, "Towards Secure Two-Party Computation from the Wire-Tap Channel," *ArXiv e-prints*, Jun. 2013.

[6] G. Cohen, S. Mesnager, and A. Patey, "On minimal and quasi-minimal linear codes," *Proceedings of Fourteenth International Conference on Cryptography and Coding, Oxford, United Kingdom, IMACC 2013, LNCS 8308 Springer, Heidelberg*, pp. 85–98, 2013.

[7] G. D. Cohen and A. Lempel, "Linear intersecting codes," *Discrete Mathematics*, vol. 56, no. 1, pp. 35–43, 1985.

[8] G. D. Cohen, S. B. Encheva, S. Litsyn, and H. G. Schaathun, "Intersecting codes and separating codes," *Discrete Applied Mathematics*, vol. 128, no. 1, pp. 75–83, 2003.

[9] G. Brassard, C. Crépeau, and M. Santha, "Oblivious transfers and intersecting codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1769–1780, 1996.

[10] A. E. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2010–2017, 1998.

[11] H.-G. Schaathun, "The Boneh-Shaw fingerprinting scheme is better than we thought," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 248–255, 2006.

[12] F. J. MacWilliams and N. J. Sloane, *The theory of error-correcting codes*. Amsterdam, North Holland, 1977.

[13] M. A. Tsfasman and S. G. Vladut, *Algebraic Geometric Codes*. Kluwer, 1991.

[14] B. Segre and U. Bartocci, "Ovali ed altre curve nei piani di Galois di caratteristica due," *Acta Arith.18 (1)*, pp. 423–449, 1971.

[15] A. Maschietti, "Difference sets and hyperovals," *Des.CodesCryptogr.14(1)*, pp. 89–98, 1998.

[16] S. Mesnager, "Bent vectorial functions and linear codes from o-polynomials," *Preprint*, 2013.

[17] C. Carlet and S. Mesnager, "On Dillon's class H of bent functions, Niho bent functions and o-polynomials," *Journal of Combinatorial Theory, Series A, Vol 118, no. 8*, pp. 2392–2410, 2011.