# MINIMAL LINEAR CODES IN ODD CHARACTERISTIC 

DANIELE BARTOLI AND MATTEO BONINI


#### Abstract

In this paper we generalize constructions in two recent works of Ding, Heng, Zhou to any field $\mathbb{F}_{q}, q$ odd, providing infinite families of minimal codes for which the Ashikhmin-Barg bound does not hold.


Keywords: Minimal codes; linear codes; secret sharing schemes
MSC 2010 Codes: 94B05, 94C10, 94A60

## 1. Introduction

Let $\mathcal{C}$ be a linear code. A codeword $c \in \mathcal{C}$ is said a minimal codeword if its support (i.e. the set of non-zero coordinates) determines $c$ up to a scalar factor. Equivalently, the support of $c$ does not contain the support of any other independent codeword.

Minimal codewords can be used [15, 16] in linear codes-based access structures in secret sharing schemes (SSS), that is protocols which include a distribution algorithm and a reconstruction algorithm, implemented by a dealer and some participants; see [3, 17]. The dealer splits a secret $s$ into different pieces (shares) and distributes them to participants $\mathcal{P}$. Only authorized subsets of $\mathcal{P}$ (access structure $\Gamma$ ) can be able to reconstruct the secret by using their respective shares. A set of participants $A$ is called a minimal authorized subsets if $A \in \Gamma$ and no proper subset of $A$ belongs to $\Gamma$. An SSS is called perfect if only authorized sets of participants can recover the secret and ideal if the shares are of the same size as that of the secret.

In his works Massey [15, 16] used linear codes for a perfect and ideal SSS. Also, he pointed out the relationship between the access structure and the set of minimal codewords of the dual code of the underlying code. In particular, the access structure of the secret-sharing scheme corresponding to an $[n, k]_{q}$-code $\mathcal{C}$ is specified by the support of minimal codewords in $\mathcal{C}^{\perp}$ having 1 as first component; see [15, 16].

Given an arbitrary linear code $\mathcal{C}$, it is a hard task to determine the set of its minimal codewords even in the binary case. In fact, the knowledge of the minimal codewords is related with the complete decoding problem, which is a NP-problem even if preprocessing is allowed [2, 8]; this means that to obtain the access structures of the SSS based on general linear codes is also hard. In general this has been done only for specific classes of linear codes and this led to the study of linear codes for which every codeword is minimal; see for instance [5, 18].

Ashikhmin and Barg [1] gave a useful criterion for a linear code to be minimal.

Theorem 1.1. A linear code $\mathcal{C}$ over $\mathbb{F}_{q}$ is minimal if

$$
\begin{equation*}
\frac{w_{\min }}{w_{\max }}>\frac{q-1}{q}, \tag{1}
\end{equation*}
$$

where $w_{\min }$ and $w_{\max }$ denote the minimum and maximum nonzero Hamming weights in $\mathcal{C}$.
On the one hand, families of minimal linear codes satisfying Condition (1) have been considered in for instance [4, 9, 11, 19]. On the other hand, Condition (11) is not necessary for linear codes to be minimal. In this direction, sporadic examples of minimal codes have been presented in [7], whereas in [6] the first infinite family of minimal binary codes has been constructed by means of Boolean functions arising from simplicial complexes. More recently, families of minimal binary and ternary codes have been investigated in [10, 13].

In this paper we generalize the constructions in [10, 13] to any field $\mathbb{F}_{q}, q$ odd, providing infinite families of minimal linear codes for which Condition (1) does not hold.

## 2. Minimal codes and Secret Sharing Schemes

Let $\mathcal{C}$ be an $[n, k]_{q}$-code, that is a $k$-dimensional linear subspace of $\mathbb{F}_{q}^{n}$. The support $\operatorname{Supp}(c)$ of a codeword $c=\left(c_{1}, \ldots, c_{n}\right) \in \mathcal{C}$ is the set $\left\{i \in[1, \ldots, n]: c_{i} \neq 0\right\}$. Clearly, the Hamming weight $w(c)$ equals $|\operatorname{Supp}(c)|$ for any codeword $c \in \mathcal{C}$.
Definition 2.1. [15] A codeword $c \in \mathcal{C}$ is minimal if it only covers the codewords $\lambda c$, with $\lambda \in \mathbb{F}_{q}^{*}$, that is

$$
\forall c^{\prime} \in \mathcal{C} \Longrightarrow\left(\operatorname{Supp}(c) \subset \operatorname{Supp}\left(c^{\prime}\right) \Longrightarrow \exists \lambda \in \mathbb{F}_{q}: c^{\prime}=\lambda c\right)
$$

Definition 2.2. [12] The code $\mathcal{C}$ is minimal if every non-zero codeword $c \in \mathcal{C}$ is minimal.
Let $G \in \mathbb{F}_{q}^{k \times n}$ be the generator matrix of $\mathcal{C}$ with columns $G_{1}, \ldots, G_{n}$ and suppose that no $G_{i}$ is the 0 -vector. The code $\mathcal{C}$ can be used to construct secret sharing schemes in the following way. The secret is an element of $\mathbb{F}_{q}$ and the set of participants $\mathcal{P}=\left\{P_{2}, \ldots, P_{n}\right\}$. The dealer chooses randomly $u=\left(u_{1}, \ldots, u_{k}\right) \in \mathbb{F}_{q}^{k}$ such that $s=u \cdot G_{1}$ and computes the corresponding codeword $v=\left(v_{1}, \ldots, v_{n}\right)=$ $u G$. Each participant $P_{i}, i \geq 2$, receives the share $v_{i}$. A set of participants $\left\{P_{i_{1}}, \ldots, P_{i_{\ell}}\right\}$ determines the secret if and only if $G_{1}$ is a linear combination of $G_{i_{1}}, \ldots, G_{i_{\ell}}$; see [15]. There is a one-to-one correspondence between minimal authorized subsets and the set of minimal codewords of the dual code $\mathcal{C}^{\perp}$.

## 3. A family of minimal codes violating the Ashikhmin-Barg bound

3.1. Notations and definition of the code $\mathcal{C}_{f}$. Let $q=p^{h}, p$ odd prime, $h \geq 1$, and consider the Galois field $\mathbb{F}_{q}$. Fix an integer $m>3$ and consider $k \in[2, \ldots, m-2]$. Choose $\alpha_{i}, i=1, \ldots, k$, to be (not necessarily distinct) elements of $\mathbb{F}_{q}^{*}$. Let us denote $(0, \ldots, 0) \in \mathbb{F}_{q}^{m}$ by $\overline{0}$.

The weight $w(x)$ of a vector $x=\left(x_{1}, \ldots, x_{m}\right) \in \mathbb{F}_{q}^{m}$ is defined as $\left|\left\{i \in[1, \ldots, m]: x_{i} \neq 0\right\}\right|$.
Consider the function $f: \mathbb{F}_{q}^{m} \backslash\{\overline{0}\} \rightarrow \mathbb{F}_{q}$ defined by

$$
f(x)= \begin{cases}\alpha_{i}, & w(x)=i  \tag{2}\\ 0, & w(x)>k\end{cases}
$$

for any $x \in \mathbb{F}_{q^{m}} \simeq \mathbb{F}_{q}^{m}, x \neq 0$.
We define the code $\mathcal{C}_{f}$ as

$$
\begin{equation*}
\mathcal{C}_{f}=\left\{(u f(x)+v \cdot x)_{x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}}: u \in \mathbb{F}_{q}, v \in \mathbb{F}_{q}^{m}\right\} \tag{3}
\end{equation*}
$$

where $v \cdot x$ denotes the usual inner product in $\mathbb{F}_{q}^{m}$ between $v=\left(v_{1}, \ldots, v_{m}\right)$ and $x=\left(x_{1}, \ldots, x_{m}\right)$.
As a notation, for any pair $(u, v) \in \mathbb{F}_{q} \times \mathbb{F}_{q}^{m}$ let $c(u, v)=(u f(x)+v \cdot x)_{x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}}$ denote the corresponding codeword of $\mathcal{C}_{f}$. Choose any ordering in $\mathbb{F}_{q}^{m} \backslash\{\overline{0}\}$. For an $x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}$, we denote by $c(u, v)_{x}$ the entry in $c(u, v)$ corresponding to $x$. The support $\operatorname{Supp}(c(u, v))$ of a codeword $c(u, v)$ is defined as the set of $\left\{x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}: c(u, v)_{x} \neq 0\right\}$.

Finally, let $\operatorname{AG}(m, q)$ be the affine space of dimension $m$ over the field $\mathbb{F}_{q}$. A hyperplane in $\mathrm{AG}(m, q)$ is an affine subspace of dimension $m-1$. For a more detailed introduction on affine spaces over finite fields we refer the reader to [14].
3.2. The minimality of the code $\mathcal{C}_{f}$. Observe that, for any fixed pair $(u, v) \in \mathbb{F}_{q} \times \mathbb{F}_{q}^{m}$, the elements $x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}$ for which the codeword $c(u, v)_{x}=0$ are contained in the union of $k+1$ hyperplanes $H(v)$ and $L_{i}(u, v), i=1, \ldots, k$, defined by

$$
\begin{equation*}
H(v)=\left\{\left(y_{1}, \ldots, y_{m}\right) \in \mathbb{F}_{q}^{m}: \sum_{j=1}^{m} v_{j} y_{j}=0\right\}, \quad L_{i}(u, v)=\left\{\left(y_{1}, \ldots, y_{m}\right) \in \mathbb{F}_{q}^{m}: \sum_{j=1}^{m} v_{j} y_{j}=-\alpha_{i} u\right\} \tag{4}
\end{equation*}
$$

More precisely,

$$
\overline{\operatorname{Supp}}(c(u, v))=\mathbb{F}_{q}^{m} \backslash(\operatorname{Supp}(c(u, v)) \cup\{\overline{0}\})=\left\{x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}: c(u, v)_{x}=0\right\}
$$

equals $\bar{H}(v) \cup \bigcup_{i=1}^{k} \bar{L}_{i}(u, v)$, where

$$
\begin{aligned}
\bar{H}(v) & =\left\{\left(y_{1}, \ldots, y_{m}\right) \in H(v): w\left(y_{1}, \ldots, y_{m}\right)>k\right\} \\
\bar{L}_{i}(u, v) & =\left\{\left(y_{1}, \ldots, y_{m}\right) \in L_{i}(u, v): w\left(y_{1}, \ldots, y_{m}\right)=i\right\}
\end{aligned}
$$

Proposition 3.1. Let $H(v)$ and $H\left(v^{\prime}\right), v, v^{\prime} \neq \overline{0}$, be two distinct hyperplanes defined as in (4). Then there exist $A, B \in \mathbb{F}_{q}^{m}$ with $w(A), w(B)>k$ such that $A \in H(v) \backslash H\left(v^{\prime}\right)$ and $B \in H\left(v^{\prime}\right) \backslash H(v)$.
Proof. It is enough to prove that, for any two distinct hyperplanes of type $H(z)$ and $H\left(z^{\prime}\right)$,

$$
\left|\left\{\left(y_{1}, \ldots, y_{m}\right) \in H(z): w\left(y_{1}, \ldots, y_{m}\right)>k\right\}\right|>q^{m-2}=\left|H(z) \cap H\left(z^{\prime}\right)\right|
$$

In fact, for a given $v=\left(v_{1}, \ldots, v_{m}\right)$, we can suppose that $v_{m}=1$ and therefore $H(v)=\left\{\left(y_{1}, \ldots, y_{m}\right) \in\right.$ $\left.\mathbb{F}_{q}^{m}: y_{m}=-\sum_{j=1}^{m-1} v_{j} y_{j}\right\}$. So,

$$
\begin{gathered}
\left|\left\{\left(y_{1}, \ldots, y_{m}\right) \in H(v): w\left(y_{1}, \ldots, y_{m}\right)>k\right\}\right| \\
\geq\left|\left\{\left(y_{1}, \ldots, y_{m}\right) \in H(v): w\left(y_{1}, \ldots, y_{m-1}\right)>k, y_{m}=-\sum_{j=1}^{m-1} v_{j} y_{j}\right\}\right|
\end{gathered}
$$

$$
\geq \sum_{j=k+1}^{m-1}\binom{m-1}{j}(q-1)^{j} \geq(q-1)^{m-1}>q^{m-2}
$$

Theorem 3.2. The code $\mathcal{C}_{f}$ is minimal.
Proof. Let $c(u, v)$ and $c\left(u^{\prime}, v^{\prime}\right)$ be two codewords, with $c(u, v) \neq \lambda c\left(u^{\prime}, v^{\prime}\right)$ for any $\lambda \in \mathbb{F}_{q}^{*}$, and both $c(u, v), c\left(u^{\prime}, v^{\prime}\right)$ different from the 0-codeword.

Suppose that $\operatorname{Supp}\left(c\left(u^{\prime}, v^{\prime}\right)\right) \subset \operatorname{Supp}(c(u, v))$, that is $\overline{\operatorname{Supp}}(c(u, v)) \subset \overline{\operatorname{Supp}}\left(c\left(u^{\prime}, v^{\prime}\right)\right)$.

- Suppose $v=\overline{0}$. Then $u \neq 0$ and $\overline{\operatorname{Supp}}(c(u, v))$ consists of all $x \in \mathbb{F}_{q}^{m}$ with $w(x)>k$. Since $\overline{\operatorname{Supp}}(c(u, v)) \subset \overline{\operatorname{Supp}}\left(c\left(u^{\prime}, v^{\prime}\right)\right), v^{\prime}=\overline{0}$. It is easily seen that $c(u, \overline{0})=\lambda c\left(u^{\prime}, \overline{0}\right)$ for some $\lambda \in \mathbb{F}_{q}$, a contradiction.
- Suppose $v^{\prime}=\overline{0}$. Then $u^{\prime} \neq 0$ and $\overline{\operatorname{Supp}}\left(c\left(u^{\prime}, v^{\prime}\right)\right)$ consists of all $x \in \mathbb{F}_{q}^{m}$ with $w(x)>k$. If $v \neq \overline{0}$ then $\overline{\operatorname{Supp}}(c(u, v))$ would also contain some $x \in \mathbb{F}_{q}^{m}$ with $0<w(x) \leq k$, a contradiction to $\overline{\operatorname{Supp}}(c(u, v)) \subset \overline{\operatorname{Supp}}\left(c\left(u^{\prime}, v^{\prime}\right)\right)$. So $v=\overline{0}$ and therefore $c(u, \overline{0})=\lambda c\left(u^{\prime}, \overline{0}\right)$ for some $\lambda \in \mathbb{F}_{q}$, a contradiction.
- Suppose $v, v^{\prime} \neq \overline{0}$. By Proposition 3.1, $H(v)=H\left(v^{\prime}\right)$, that is $v=\lambda v^{\prime}$ for some $\lambda \in \mathbb{F}_{q}^{*}$. Also, $L_{i}(u, v) \subset L_{i}\left(u^{\prime}, v^{\prime}\right)=L_{i}\left(u^{\prime}, \lambda v\right)$, for any $i=1, \ldots, k$. Since $L_{i}(u, v)$ and $L_{i}\left(u^{\prime}, \lambda v\right)$ can be either disjoint or coincident, $u^{\prime}=\lambda u$ and therefore $c\left(u^{\prime}, v^{\prime}\right)=\lambda c(u, v)$, a contradiction.
Then $\operatorname{Supp}\left(c\left(u^{\prime}, v^{\prime}\right)\right) \not \subset \operatorname{Supp}(c(u, v))$ and $\mathcal{C}_{f}$ is minimal.


### 3.3. The parameters of $\mathcal{C}_{f}$.

Proposition 3.3. The code $\mathcal{C}_{f}$ has length $q^{m}-1$ and dimension $m+1$ over $\mathbb{F}_{q}$. If

$$
\begin{equation*}
q^{m}-1-\sum_{i=1}^{m-1}\binom{m-1}{i}(q-1)^{i}-\sum_{i=1}^{k}\binom{m-1}{i}(q-1)^{i} \geq \sum_{i=1}^{k}\binom{m}{i}(q-1)^{i} \tag{5}
\end{equation*}
$$

then minimum and maximum weights in $\mathcal{C}_{f}$ satisfy

$$
w_{\min }=\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i}, \quad w_{\max } \geq q^{m}-q^{m-1}
$$

Also, if

$$
\begin{equation*}
\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i-1} \leq q^{m-1}-q^{m-2} \tag{6}
\end{equation*}
$$

then $w_{\min } / w_{\max } \leq(q-1) / q$.
Proof. Clearly, the length of $\mathcal{C}_{f}$ is $\left|\mathbb{F}_{q}^{m} \backslash\{\overline{0}\}\right|=q^{m}-1$.
Each codeword in $\mathcal{C}_{f}$ can be written as linear combination of $c(1, \overline{0}), c\left(0, e_{1}\right), \ldots, c\left(0, e_{m}\right)$, where $e_{1}, \ldots, e_{m}$ is the standard basis of $\mathbb{F}_{q}^{m}$ over $\mathbb{F}_{q}$.

On the other hand, suppose that $c(u, v)$ is the zero codeword.

- If $u=0$, then for elements $y_{i}=e_{i} \in \mathbb{F}_{q}^{m}, i=1, \ldots, m$, we have $c(u, v)_{y_{i}}=v_{i}=0$, and then $v=\overline{0}$.
- If $u \neq 0$, then we can consider $y_{i}=e_{i}, i=1, \ldots, m$ and $y=2 e_{i}$ and then $c(u, v)_{y_{i}}=u \alpha_{1}+v_{i}=0$, $c(u, v)_{2 y_{i}}=u \alpha_{1}+2 v_{i}=0$. Since $\alpha_{1} \neq 0$ (see (2)), the above conditions yield $v_{1}=\cdots=v_{m}=$ $u=0$.

This proves that $c(1, \overline{0}), c\left(0, e_{1}\right), \ldots, c\left(0, e_{m}\right)$ is a basis of $\mathcal{C}$ of size $m+1$.
We now determine the minimum weight of the code. Recall that for a codeword $c(u, v)$ its weight is

$$
w(c(u, v))=\mid \operatorname{Supp}\left((c(u, v))\left|=q^{m}-1-\right| \overline{\operatorname{Supp}}((c(u, v)) \mid .\right.
$$

- The codeword $c(0, \overline{0})$ is the 0 -codeword.
- The $q-1$ codewords $c(u, \overline{0}), u \neq 0$, have weight exactly $\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i}$. In fact, $c(u, \overline{0})_{x}=$ $\alpha_{w(x)} u$ is non-zero if and only if $w(x) \in[1, \ldots, k]$.
- The $q^{m}-1$ codewords $c(0, v), v \neq \overline{0}$, have weight exactly $q^{m}-q^{m-1}$, since each $x \in \mathbb{F}_{q}^{m} \backslash\{\overline{0}\}$ satisfying $v \cdot x=0$ belongs to $\overline{\operatorname{Supp}}(c(0, v))$.
- For a codeword $c(u, v)$, with $u \neq 0$ and $v \neq \overline{0}$,

$$
\overline{\operatorname{Supp}}(c(u, v))=\bar{H}(v) \cup \bigcup_{i=1}^{k} \bar{L}_{i}(u, v)
$$

see Proposition 4. Without loss of generality we can suppose that $v_{m}=1$. We have that

$$
\begin{array}{r}
\sum_{i=k+1}^{m-1}\binom{m-1}{i}(q-1)^{i}=\left|\left\{\left(x_{1}, \ldots, x_{m}\right): x_{m}=-\sum_{j=1}^{m-1} v_{j} x_{j}, w\left(x_{1}, \ldots, x_{m-1}\right) \geq k+1\right\}\right| \leq \\
|\bar{H}(v)| \leq\left|\left\{\left(x_{1}, \ldots, x_{m}\right): x_{m}=-\sum_{j=1}^{m-1} v_{j} x_{j}, w\left(x_{1}, \ldots, x_{m-1}\right) \geq k\right\}\right|= \\
\sum_{i=k}^{m-1}\binom{m-1}{i}(q-1)^{i}
\end{array}
$$

Analogously,

$$
\begin{aligned}
& 0 \leq\left|\bar{L}_{i}(u, v)\right| \leq \mid\left\{\left(x_{1}, \ldots, x_{m}\right): x_{m}=-f(x) u\right.\left.-\sum_{j=1}^{m-1} v_{j} x_{j}, w\left(x_{1}, \ldots, x_{m-1}\right) \in[i-1, i]\right\} \mid= \\
& \leq\binom{ m-1}{i-1}(q-1)^{i-1}+\binom{m-1}{i}(q-1)^{i}
\end{aligned}
$$

Thus,

$$
\sum_{i=k+1}^{m-1}\binom{m-1}{i}(q-1)^{i} \leq|\overline{\operatorname{Supp}}(c(u, v))| \leq \sum_{i=1}^{m-1}\binom{m-1}{i}(q-1)^{i}+\sum_{i=1}^{k}\binom{m-1}{i}(q-1)^{i}
$$

and

$$
\begin{gathered}
q^{m}-1-\sum_{i=1}^{m-1}\binom{m-1}{i}(q-1)^{i}-\sum_{i=1}^{k}\binom{m-1}{i}(q-1)^{i} \leq \\
w(c(u, v)) \leq q^{m}-1-\sum_{i=k+1}^{m-1}\binom{m-1}{i}(q-1)^{i} .
\end{gathered}
$$

By (5), the minimum weight is

$$
w_{\min }=\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i}
$$

whereas

$$
w_{\max } \geq q^{m}-q^{m-1}
$$

Finally, if (6) holds,

$$
\frac{w_{\min }}{w_{\max }}=\frac{\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i}}{q^{m}-q^{m-1}} \leq \frac{q-1}{q} .
$$

Remark 3.4. Note that if (5) does not hold, then $w_{\min } \leq \sum_{i=1}^{k}\binom{m}{i}(q-1)^{i}$. Arguing as in Proposition 3.3. Condition (6) yields $w_{\min } / w_{\max } \leq(q-1) / q$.

Corollary 3.5. If $q \geq 5,2<m \leq q-1$, and $k \leq(m-1) / 2$ then Conditions (5) and (6) hold. Proof. First of all observe that

$$
\begin{gathered}
\sum_{i=1}^{m-1}\binom{m-1}{i}(q-1)^{i}=q^{m-1}-1, \\
\sum_{i=0}^{\alpha}\binom{m}{i}(q-1)^{i} \leq \sum_{i=0}^{\alpha} m^{i} q^{i} \leq 2 q^{2 \alpha} \\
\sum_{i=0}^{\alpha}\binom{m}{i}(q-1)^{i-1} \leq \sum_{i=0}^{\alpha} m^{i} q^{i-1} \leq 2 q^{2 \alpha-1}
\end{gathered}
$$

Therefore we have that

$$
\begin{aligned}
q^{m}-1-\sum_{i=1}^{m-1}\binom{m-1}{i}(q-1)^{i}-\sum_{i=1}^{k}\binom{m-1}{i}(q-1)^{i}-\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i} & \geq \\
q^{m}-1-q^{m-1}+1-2 q^{2 k}-2 q^{2 k} & \geq \\
q^{m}-5 q^{m-1} & \geq 0
\end{aligned}
$$

and Condition (5) holds.
Also,

$$
\sum_{i=1}^{k}\binom{m}{i}(q-1)^{i-1} \leq \sum_{i=1}^{k} m^{i}(q-1)^{i-1} \leq \sum_{i=1}^{k} q^{2 i-1} \leq 2 q^{2 k-1} \leq 2 q^{m-2} \leq q^{m-1}-q^{m-2}
$$

and Condition (6) is satisfied.

## 4. Acknowledgments

The research of D. Bartoli was supported by Ministry for Education, University and Research of Italy (MIUR) (Project "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

The research of M. Bonini was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

## References

[1] A. Ashikhmin, A. Barg. Minimal vectors in linear codes. IEEE Trans. Inf. Theory 44(5) (1998) 2010-2017.
[2] E.R Berlekamp, R.J. McEliece, H.C.A. van Tilborg. On the Inherent Intractability of Certain Coding Problems. In: IEEE Trans. Inform. Theory, IT-24, no. 3, (1978), 384-386.
[3] G.R. Blakley. Safeguarding cryptographic keys. In: Proceedings of AFIPS National Computer Conference. New York, USA, AFIPS Press 48(1979) 313-317.
[4] C. Carlet, C. Ding, J. Yuan. Linear codes from highly nonlinear functions and their secret sharing schemes. IEEE Trans. Inf. Theory 51(6) (2005) 2089-2102.
[5] H. Chabanne, G. Cohen, A. Patey. Towards Secure Two-Party Computation from the Wire-Tap Channel. In: Information Security and Cryptology - ICISC 2013, pp. 34-46. Springer, Heidelberg, 2014.
[6] S. Chang, J. Y. Hyun. Linear codes from simplicial complexes. Des. Codes Cryptogr. DOI: https://link.springer.com/article/10.1007/s10623-017-0442-5 (2017).
[7] G.D. Cohen, S. Mesnager, A. Patey. On minimal and quasi-minimal linear codes. In: M. Stam (Ed.), IMACC 2013, LNCS vol. 8308, pp. 85-98, Springer, Heidelberg, 2013.
[8] J. Bruck, M. Naor. The Hardness of Decoding Linear Codes with Preprocessing. In: IEEE Trans. Inform. Theory 36(2) (1990).
[9] C. Ding. Linear codes from some 2-designs. IEEE Trans. Inf. Theory 60(6) (2015) 3265-3275.
[10] C. Ding, Z. Heng, Z. Zhou. Minimal binary linear codes. IEEE Trans. Inf. Theory, DOI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=\&arnumber=8325311\&tag=1.
[11] C. Ding, N. Li, C. Li, Z. Zhou. Three-weight cyclic codes and their weight distributions. Discrete Mathematics 39 (2016) 415-427.
[12] C. Ding, J. Yuan. 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).
[13] Z. Heng, C. Ding, X. Zhou. Minimal Linear Codes over Finite Fields. https://arxiv.org/pdf/1803.09988.pdf.
[14] J.W.P. Hirschfeld. Projective geometries over finite fields, second edition. Oxford Univ. Press, Oxford, (1998).
[15] J.L. Massey. Minimal codewords and secret sharing. In: Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory, pp. 276-279 (1993)
[16] J.L. Massey. 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] A. Shamir. How to share a secret. Communications of the ACM 24 (1979) 612-613.
[18] Y. Song, Z. Li. Secret sharing with a class of minimal linear codes. https://arxiv.org/abs/1202.4058 (2012)
[19] J. Yuan, C. Ding. Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory $\mathbf{5 2}$ (1) (2006) 206-212.

Department of Mathematics and Informatics, University of Perugia, Perugia, Italy
E-mail address: daniele.bartoli@unipg.it
Department of Mathematics, University of Trento, Trento, Italy
E-mail address: matteo.bonini@unitn.it

