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 C be a linear code. A codeword $c \in C$ 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 Γ) 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 Γ . 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 C is specified by the support of minimal codewords in C^{\perp} having 1 as first component; see [15, 16].

Given an arbitrary linear code 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 C over \mathbb{F}_q is minimal if

(1)
$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q}$$

where w_{min} and w_{max} denote the minimum and maximum nonzero Hamming weights in 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 (1) 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 Supp(c) of a codeword $c = (c_1, \ldots, c_n) \in \mathcal{C}$ is the set $\{i \in [1, \ldots, n] : c_i \neq 0\}$. Clearly, the Hamming weight w(c) equals |Supp(c)| for any codeword $c \in \mathcal{C}$.

Definition 2.1. [15] A codeword $c \in C$ is *minimal* if it only covers the codewords λc , with $\lambda \in \mathbb{F}_q^*$, that is

$$\forall c' \in \mathcal{C} \Longrightarrow (Supp(c) \subset Supp(c') \Longrightarrow \exists \lambda \in \mathbb{F}_q : c' = \lambda c).$$

Definition 2.2. [12] The code C is *minimal* if every non-zero codeword $c \in C$ 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 $\mathcal{P} = \{P_2, \ldots, P_n\}$. The dealer chooses randomly $u = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ such that $s = u \cdot G_1$ and computes the corresponding codeword $v = (v_1, \ldots, v_n) =$ uG. Each participant $P_i, i \geq 2$, receives the share v_i . A set of participants $\{P_{i_1}, \ldots, P_{i_\ell}\}$ 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 C_f . Let $q = p^h$, p odd prime, $h \ge 1$, and consider the Galois field \mathbb{F}_q . Fix an integer m > 3 and consider $k \in [2, \ldots, m-2]$. Choose α_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 $x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m$ is defined as $|\{i \in [1, \ldots, m] : x_i \neq 0\}|$. Consider the function $f : \mathbb{F}_q^m \setminus \{\overline{0}\} \to \mathbb{F}_q$ defined by

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

for any $x \in \mathbb{F}_{q^m} \simeq \mathbb{F}_q^m, x \neq 0.$

We define the code \mathcal{C}_f as

(3)
$$\mathcal{C}_f = \{ (uf(x) + v \cdot x)_{x \in \mathbb{F}_q^m \setminus \{\overline{0}\}} : u \in \mathbb{F}_q, v \in \mathbb{F}_q^m \},$$

where $v \cdot x$ denotes the usual inner product in \mathbb{F}_q^m between $v = (v_1, \ldots, v_m)$ and $x = (x_1, \ldots, x_m)$.

As a notation, for any pair $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q^m$ let $c(u, v) = (uf(x) + v \cdot x)_{x \in \mathbb{F}_q^m \setminus \{\overline{0}\}}$ denote the corresponding codeword of \mathcal{C}_f . Choose any ordering in $\mathbb{F}_q^m \setminus \{\overline{0}\}$. For an $x \in \mathbb{F}_q^m \setminus \{\overline{0}\}$, we denote by $c(u, v)_x$ the entry in c(u, v) corresponding to x. The support Supp(c(u, v)) of a codeword c(u, v) is defined as the set of $\{x \in \mathbb{F}_q^m \setminus \{\overline{0}\} : c(u, v)_x \neq 0\}$.

Finally, let AG(m, q) be the affine space of dimension m over the field \mathbb{F}_q . A hyperplane in 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 C_f . Observe that, for any fixed pair $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q^m$, the elements $x \in \mathbb{F}_q^m \setminus \{\overline{0}\}$ 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 (4)

$$H(v) = \left\{ (y_1, \dots, y_m) \in \mathbb{F}_q^m : \sum_{j=1}^m v_j y_j = 0 \right\}, \quad L_i(u, v) = \left\{ (y_1, \dots, y_m) \in \mathbb{F}_q^m : \sum_{j=1}^m v_j y_j = -\alpha_i u \right\}.$$

More precisely,

$$\overline{Supp}(c(u,v)) = \mathbb{F}_q^m \setminus \left(Supp(c(u,v)) \cup \{\overline{0}\}\right) = \left\{x \in \mathbb{F}_q^m \setminus \{\overline{0}\} : c(u,v)_x = 0\right\}$$

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

$$\overline{H}(v) = \{(y_1, \dots, y_m) \in H(v) : w(y_1, \dots, y_m) > k\},\$$

$$\overline{L}_i(u, v) = \{(y_1, \dots, y_m) \in L_i(u, v) : w(y_1, \dots, y_m) = i\}.$$

Proposition 3.1. Let H(v) and H(v'), $v, v' \neq \overline{0}$, 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 $A \in H(v) \setminus H(v')$ and $B \in H(v') \setminus H(v)$.

Proof. It is enough to prove that, for any two distinct hyperplanes of type H(z) and H(z'),

$$|\{(y_1,\ldots,y_m)\in H(z) : w(y_1,\ldots,y_m)>k\}|>q^{m-2}=|H(z)\cap H(z')|.$$

In fact, for a given $v = (v_1, \ldots, v_m)$, we can suppose that $v_m = 1$ and therefore $H(v) = \{(y_1, \ldots, y_m) \in \mathbb{F}_q^m : y_m = -\sum_{j=1}^{m-1} v_j y_j\}$. So,

$$\left| \left\{ (y_1, \dots, y_m) \in H(v) : w(y_1, \dots, y_m) > k \right\} \right|$$

$$\geq \left| \left\{ (y_1, \dots, y_m) \in H(v) : w(y_1, \dots, y_{m-1}) > k, y_m = -\sum_{j=1}^{m-1} v_j y_j \right\} \right|$$

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

Theorem 3.2. The code C_f is minimal.

Proof. Let c(u, v) and c(u', v') be two codewords, with $c(u, v) \neq \lambda c(u', v')$ for any $\lambda \in \mathbb{F}_q^*$, and both c(u, v), c(u', v') different from the 0-codeword.

Suppose that $Supp(c(u', v')) \subset Supp(c(u, v))$, that is $\overline{Supp}(c(u, v)) \subset \overline{Supp}(c(u', v'))$.

- Suppose $v = \overline{0}$. Then $u \neq 0$ and $\overline{Supp}(c(u, v))$ consists of all $x \in \mathbb{F}_q^m$ with w(x) > k. Since $\overline{Supp}(c(u, v)) \subset \overline{Supp}(c(u', v')), v' = \overline{0}$. It is easily seen that $c(u, \overline{0}) = \lambda c(u', \overline{0})$ for some $\lambda \in \mathbb{F}_q$, a contradiction.
- Suppose $v' = \overline{0}$. Then $u' \neq 0$ and $\overline{Supp}(c(u', v'))$ consists of all $x \in \mathbb{F}_q^m$ with w(x) > k. If $v \neq \overline{0}$ then $\overline{Supp}(c(u, v))$ would also contain some $x \in \mathbb{F}_q^m$ with $0 < w(x) \leq k$, a contradiction to $\overline{Supp}(c(u, v)) \subset \overline{Supp}(c(u', v'))$. So $v = \overline{0}$ and therefore $c(u, \overline{0}) = \lambda c(u', \overline{0})$ for some $\lambda \in \mathbb{F}_q$, a contradiction.
- Suppose $v, v' \neq \overline{0}$. By Proposition 3.1, H(v) = H(v'), that is $v = \lambda v'$ for some $\lambda \in \mathbb{F}_q^*$. Also, $L_i(u, v) \subset L_i(u', v') = L_i(u', \lambda v)$, for any $i = 1, \ldots, k$. Since $L_i(u, v)$ and $L_i(u', \lambda v)$ can be either disjoint or coincident, $u' = \lambda u$ and therefore $c(u', v') = \lambda c(u, v)$, a contradiction.

Then $Supp(c(u', v')) \not\subset Supp(c(u, v))$ and \mathcal{C}_f is minimal.

3.3. The parameters of C_f .

Proposition 3.3. The code C_f has length $q^m - 1$ and dimension m + 1 over \mathbb{F}_q . If

(5)
$$q^{m} - 1 - \sum_{i=1}^{m-1} {m-1 \choose i} (q-1)^{i} - \sum_{i=1}^{k} {m-1 \choose i} (q-1)^{i} \ge \sum_{i=1}^{k} {m \choose i} (q-1)^{i}$$

then minimum and maximum weights in C_f satisfy

$$w_{min} = \sum_{i=1}^{k} {m \choose i} (q-1)^{i}, \qquad w_{max} \ge q^{m} - q^{m-1}.$$

Also, if

(6)
$$\sum_{i=1}^{k} \binom{m}{i} (q-1)^{i-1} \le q^{m-1} - q^{m-2}$$

then $w_{min}/w_{max} \leq (q-1)/q$.

Proof. Clearly, the length of C_f is $|\mathbb{F}_q^m \setminus \{\overline{0}\}| = q^m - 1$.

Each codeword in C_f can be written as linear combination of $c(1,\overline{0})$, $c(0,e_1)$, ..., $c(0,e_m)$, 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, ..., m and $y = 2e_i$ and then $c(u, v)_{y_i} = u\alpha_1 + v_i = 0$, $c(u, v)_{2y_i} = u\alpha_1 + 2v_i = 0$. Since $\alpha_1 \neq 0$ (see (2)), the above conditions yield $v_1 = \cdots = v_m = u = 0$.

This proves that $c(1, \overline{0}), c(0, e_1), \ldots, c(0, e_m)$ is a basis of 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

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

- The codeword $c(0,\overline{0})$ is the 0-codeword.
- The q-1 codewords $c(u,\overline{0}), u \neq 0$, have weight exactly $\sum_{i=1}^{k} {m \choose i} (q-1)^{i}$. 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 $x \in \mathbb{F}_q^m \setminus \{\overline{0}\}$ satisfying $v \cdot x = 0$ belongs to $\overline{Supp}(c(0, v))$.
- For a codeword c(u, v), with $u \neq 0$ and $v \neq \overline{0}$,

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

see Proposition 4. Without loss of generality we can suppose that $v_m = 1$. We have that

$$\begin{split} \sum_{i=k+1}^{m-1} \binom{m-1}{i} (q-1)^i &= \left| \left\{ (x_1, \dots, x_m) : x_m = -\sum_{j=1}^{m-1} v_j x_j, \ w(x_1, \dots, x_{m-1}) \ge k+1 \right\} \right| &\leq \\ &\left| \overline{H}(v) \right| \le \left| \left\{ (x_1, \dots, x_m) : x_m = -\sum_{j=1}^{m-1} v_j x_j, \ w(x_1, \dots, x_{m-1}) \ge k \right\} \right| &= \\ &\left| \sum_{i=k}^{m-1} \binom{m-1}{i} (q-1)^i. \end{split}$$

Analogously,

$$0 \le \left|\overline{L}_{i}(u,v)\right| \le \left|\left\{(x_{1},\ldots,x_{m}) : x_{m} = -f(x)u - \sum_{j=1}^{m-1} v_{j}x_{j}, w(x_{1},\ldots,x_{m-1}) \in [i-1,i]\right\}\right| = \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1} + \binom{m-1}{i}(q-1)^{i}\right| \le \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1} + \binom{m-1}{i}(q-1)^{i}\right|\right| = \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1} + \binom{m-1}{i}(q-1)^{i}\right| \le \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1}\right| \le \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1}\right| \le \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1}\right|\right| \le \left|\left(\frac{m-1}{i-1}\right)(q-1)^{i-1}\right| \le \left|\left(\frac$$

Thus,

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

and

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

By (5), the minimum weight is

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

whereas

$$w_{max} \ge q^m - q^{m-1}.$$

Finally, if (6) holds,

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

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

Corollary 3.5. If $q \ge 5$, $2 < m \le q - 1$, and $k \le (m - 1)/2$ then Conditions (5) and (6) hold.

Proof. First of all observe that

$$\sum_{i=1}^{m-1} \binom{m-1}{i} (q-1)^i = q^{m-1} - 1,$$
$$\sum_{i=0}^{\alpha} \binom{m}{i} (q-1)^i \le \sum_{i=0}^{\alpha} m^i q^i \le 2q^{2\alpha},$$
$$\sum_{i=0}^{\alpha} \binom{m}{i} (q-1)^{i-1} \le \sum_{i=0}^{\alpha} m^i q^{i-1} \le 2q^{2\alpha-1}.$$

Therefore we have that

$$q^{m} - 1 - \sum_{i=1}^{m-1} \binom{m-1}{i} (q-1)^{i} - \sum_{i=1}^{k} \binom{m-1}{i} (q-1)^{i} - \sum_{i=1}^{k} \binom{m}{i} (q-1)^{i} \ge q^{m} - 1 - q^{m-1} + 1 - 2q^{2k} - 2q^{2k} \ge q^{m} - 5q^{m-1} \ge 0$$

and Condition (5) holds.

Also,

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

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.
- 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.
- 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 52(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