Yet another variation on minimal linear codes (extended summary)

Gérard Cohen
Télécom ParisTech
UMR 5141, CNRS
46 rue Barrault, 75013 Paris
Email: cohen@enst.fr

Sihem Mesnager
Department of Mathematics
University of Paris XIII and University of Paris VIII
LAGA, UMR 7539, CNRS, Sorbonne Paris Cité
Email: smesnager@univ-paris8.fr

Hugues Randriam
Télécom ParisTech
UMR 5141, CNRS
46 rue Barrault, 75013 Paris
Email: randriam@enst.fr

***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 consider here quasi-minimal, t-minimal, and t-quasi-minimal linear codes, which are new variations on this notion.**

Part of this work was done by the first two authors and presented at 4th International Castle Meeting on Coding Theory and Applications Palmela, Portugal, 15-18 September 2014; an extended version with all proofs has been submitted to AMC ([CMR14]).

Keywords. Linear codes, minimal codes, quasi-minimal codes.

I. Introduction and notation

A *minimal codeword* [Mas93], [Mas95] 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 some secret sharing schemes. This led to work on how to find codes where all codewords are minimal. The problem of finding a code satisfying this condition, called a *minimal linear code* has first been envisioned in [DY03] and later studied in [SL12], [CCP13]. In [CCP13], another motivation is a new proposal for secure two-party computation, where it is required that minimal linear codes be used to ensure privacy. Minimal codes are close to the notions of intersecting and separating codes [CL85], [CELS03], [Ran13a], hashing and parent-identifying codes [ACKL03], [CS04]. Such codes have been suggested for applications to oblivious transfer [BCS96], secret sharing [ABCH95], [AB98], [DY03], [SL12] broadcast encryption or digital fingerprinting [Sch06].

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

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

II. t-minimal and t-quasi-minimal codes

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

A. Definition and properties

Definition 1.
- *A codeword c is t-minimal if:* $\forall c' \in C, (|supp(c') \setminus supp(c)| < t) \implies c' \in \mathbb{F}_q \cdot c$.
- *A codeword c is t-quasi-minimal if:* $\forall c' \in C, (|supp(c') \triangle supp(c)| < t) \implies c' \in \mathbb{F}_q^\times \cdot c$.

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

Note that for $t = 1$ this definition reduces to the notions of minimality and quasi-minimality previously considered in [CMP13]. It also makes sense when c is the zero codeword.

Definition 2. *A linear code C is t-minimal (resp. t-quasi-minimal) if every codeword $c \in C$ is t-minimal (resp. t-quasi-minimal).*

Proposition 3. *We have the following diagram of implications between properties of C:*

$$\begin{tikzcd}
t\text{-minimal} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{minimal} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{intersecting} \\
t\text{-quasi-minimal} \arrow[r, Rightarrow] & \text{quasi-minimal} \arrow[ur, Rightarrow, "q>2"] &
\end{tikzcd}$$

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

B. (Asymptotic) lower bounds

Theorem 4. *Suppose $\tau < \frac{q-1}{q^2}$ and*

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

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

Theorem 5. *Suppose $\tau < \frac{2q-2}{q^2}$ and*

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

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

C. A construction

Proposition 6. *Let C_1 be t_1-minimal (resp. t_1-quasi-minimal) and C_2 be t_2-minimal (resp. t_2-quasi-minimal). Then $C_1 \otimes C_2$ is t_1t_2-minimal (resp. t_1t_2-quasi-minimal).*

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

First we deal with minimality. Suppose

$$|supp(m') \setminus supp(m)| < t_1t_2.$$

Set

$$I = \{i;\ |supp(r'^i) \setminus supp(r^i)| \geq t_2\},$$

$$J = \{j;\ |supp(c'^j) \setminus supp(c^j)| \geq t_1\}.$$

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

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

To conclude it suffices to show all λ_i with $r^i \neq 0$ are equal. So suppose $r^{i_1}, r^{i_2} \neq 0$. By Proposition 3, C_2 is intersecting, so we can choose $j \in supp(r^{i_1}) \cap supp(r^{i_2})$. Then, since $J = \emptyset$ and C_1 is t_1-minimal, there is $\mu_j \in \mathbb{F}_q$ such that $c'^j = \mu_j c^j$. Looking at the (i_1, j) and (i_2, j) entries, this gives $\lambda_{i_1} = \mu_j = \lambda_{i_2}$, as claimed.

Now we deal with quasi-minimality. For $q = 2$ the result is already known, since t-quasi-minimality just means minimum distance at least t. So we can suppose $q > 2$. We then proceed exactly as above, with symmetric difference $\triangle$ replacing ordinary set difference $\setminus$, and with the λ_i in $\mathbb{F}_q^\times$ instead of $\mathbb{F}_q$. In the last step we will need C_2 to be intersecting, which is true for $q > 2$ by Proposition 3 again. ∎

D. A sufficient condition

Theorem 7. *Let C be a linear $[n, k, d, d_{max}]_q$ code;*

if $(q-1)d > (q-2)d_{max} + q(t-1)/2$, then C is t-quasi-minimal.

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

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

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

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

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

References

[ACKL03] N. Alon, G. Cohen, M. Krivilevitch and S. Litsyn. Generalized hashing and applications. *JCT-A* 104, pages 207–215, 2003.

[AB98] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5), pages 2010–2017, 1998.

[ABCH95] A. Ashikhmin, A. Barg, G. Cohen, and L. Huguet. Variations on minimal codewords in linear codes. *LNCS 948*, pages 96–105, 1995.

[BCS96] G. Brassard, C. Crépeau, and M. Santha. Oblivious transfers and intersecting codes. *IEEE Transactions on Information Theory*, 42(6), pages 1769–1780, 1996.

[CCP13] H. Chabanne, G. Cohen, and A. Patey. Towards Secure Two-Party Computation from the Wire-Tap Channel. *ArXiv e-prints*, June 2013.

[CELS03] G. Cohen, S. Encheva, S. Litsyn, and Hr-.G. Schaathun. Intersecting codes and separating codes. *Discrete Applied Mathematics*, 128(1), pages 75–83, 2003.

[CL85] G. Cohen, and A. Lempel. Linear intersecting codes. *Discrete Mathematics*, 56(1), pages 35–43, 1985.

[CMP13] 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*, pages 85–98, 2013.

[CMR14] G. Cohen, S. Mesnager and H. Randriam. Yet another variation on minimal linear codes. Advances in Mathematics of Communications, submitted.

[CS04] G. Cohen and H-G. Schaathun. Upper bounds on separating codes. *IEEE Transactions on Information Theory*, 50, pages 1291–1295, 2004.

[DY03] C. Ding and J. Yuan. Covering and secret sharing with linear codes. *DMTCS*, volume 2731, *Lecture Notes in Computer Science*, pages 11–25. Springer DMTCS, 2003.

[Mas93] J.L. Massey. Minimal codewords and secret sharing. In *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory*, pages 276–279, 1993.

[Mas95] J.L. Massey. Some applications of coding theory in cryptography. In P. G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, pages 33–47. Formara Ltd, 1995.

[MS77] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*. Amsterdam, North Holland, 1977.

[Ran13a] H. Randriambololona. $(2, 1)$-separating systems beyond the probabilistic bound. *Israel Journal of Mathematics*, 195(1), pages 171–186, 2013.

[Ran13b] H. Randriambololona. Asymptotically good binary linear codes with asymptotically good self-intersection spans. *IEEE Transactions on Information Theory*, 59(5), pages 3038–3045, 2013.

[Ran15] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. *To appear in Contemporary Mathematics*, 637, 2015.

[Sch06] H.G. Schaathun. The Boneh-Shaw fingerprinting scheme is better than we thought. *IEEE Transactions on Information Forensics and Security*, 1(2), pages 248–255, 2006.

[SL12] Y. Song and Z. Li. Secret sharing with a class of minimal linear codes. *CoRR*, abs/1202.4058, 2012.