The Main Conjecture for Near-MDS Codes

Ivan Landjev, Assia Rousseva

▶ To cite this version:

Ivan Landjev, Assia Rousseva. The Main Conjecture for Near-MDS Codes. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Anne Canteaut, Gaëtan Leurent, Maria Naya-Plasencia, Apr 2015, Paris, France. hal-01276222

HAL Id: hal-01276222

https://inria.hal.science/hal-01276222

Submitted on 19 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The Main Conjecture for Near-MDS Codes

Ivan Landjev[1] and Assia Rousseva[2]

[1] New Bulgarian University, 21 Montevideo str., Sofia 1618, Bulgaria
i.landjev@nbu.bg
[2] Sofia University, 5 J. Bourchier blvd., 1126 Sofia, Bulgaria
assia@fmi.uni-sofia.bg

Keywords: near-MDS codes, MDS codes, elliptic curves, $(n, 3)$-arcs, n-tracks, projective geometries

1 Introduction

Near-MDS have been introduced in 1995 in [11]. They are defined by weakening some restrictions in the definition of the MDS codes. The most popular definition is via generalized Hamming weights. A linear $[n, k]_q$-code C is called a near-MDS code if

$$d_i(C) = n - k + 1 \text{ for } i = 2, \dots, k, \;\; d_1(C) = n - k.$$

Of course, it is enough to require $d_1(C) = n-k$ and $d_2(C) = n-k+2$. From the properties of the generalized Hamming weights one can easily deduce that the dual of a near-MDS code is again a near-MDS code. The following propositions characterize near-MDS codes and can serve as alternative definitions. The proofs can be found in [11].

Proposition 1. *A linear $[n, k]_q$-code C is a near-MDS code if and only if any parity-check matrix H_C of C satisfies the conditions:*

(1) any $n - k - 1$ columns of H_C are linearly independent;
(2) there exist $n - k$ linearly dependent columns;
(3) any $n - k + 1$ columns of H_C are of rank $n - k$.

Proposition 2. *A linear $[n, k]_q$-code C is near-MDS if and only if any generator matrix G_C of C satisfies the conditions:*

(1) any $k - 1$ columns of G_C are linearly independent;
(2) there exist k linearly dependent columns;
(3) any $k + 1$ columns of G_C are of rank k.

Proposition 3. *A linear $[n, k]_q$ code is a near-MDS code if and only if $d(C) + d(C^{\perp}) = n$.*

Closely related to near-MDS codes are the so-called almost-MDS codes introduced by de Boer [8,9]. Almost-MDS are defined as $[n,k]_q$-codes with minimum distance $d = n - k$, or, in other words, as codes with Singleton defect 1. Not every almost-MDS code is near-MDS, as pointed out in [11], but for large n both notions coincide.

Proposition 4. *If $n > k + q$ every $[n,k,n-k]_q$-code is a near-MDS code.*

The weight distribution of a near-MDS code can be determined up to a single parameter. In the theorem below it is taken to be the number of words of minimal weight.

Theorem 1. *Let C be an $[n,k]_q$ near-MDS code. Let (A_i) and (A'_i) be the spectra of C and $C^{\perp}$, respectively. Then*

$$A_{n-k+s} = \binom{n}{k-s} \sum_{j=0}^{s-1} (-1)^j \binom{n-k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{k}{s} A_{n-k},$$

where $s = 1, \ldots, k$, and

$$A'_{k+s} = \binom{n}{k+s} \sum_{j=0}^{s-1} (-1)^j \binom{k+s}{j} (q^{s-j} - 1) + (-1)^s \binom{n-k}{s} A'_k,$$

where $s = 1, \ldots, n-k$.

For almost-MDS codes the situation is more complicated. The numbers of the parameters depends on the Singleton defect of the orthogonal code (cf. [16]). Theorem 1 gives a simple upper bound on the number of words of minimal weight.

Corollary 1. *For an $[n,k]_q$ near-MDS code*

$$A_{n-k} \leq \binom{n}{k-1} \frac{q-1}{k},$$

with equality if and only if $A_{n-k+1} = 0$. By duality,

$$A'_k \leq \binom{n}{k+1} \frac{q-1}{n-k},$$

with equality if and only if $A'_{k+1} = 0$.

2 The Geometric View at Near-MDS Codes

It is known that with every $[n, k, d]_q$-code of full length one can associate a multiset of points in $\mathrm{PG}(k-1, q)$ (possibly in a non-unique way) so that isomorphic codes are associated with projectively equivalent multisets (cf. [14]). This implies that the existence of an $[n, k]_q$ near-MDS code is equivalent to that of a set $\mathcal{K}$ of points in $\mathrm{PG}(k-1, q)$ with the following properties:

(1) every $k-1$ points from $\mathcal{S}$ are in general position (generate a hyperplane)
(2) there exist k points from $\mathcal{S}$ that lie in a hyperplane
(3) every $k+1$ points from $\mathcal{S}$ generate $\mathrm{PG}(k-1, q)$.

In particular, if $k = 3$ a near-MDS code is equivalent to an $(n, 3)$-arc in $\mathrm{PG}(2, q)$. The nonexistence of maximal $(n, 3)$-arcs, i.e. arcs with $n = 2q + 3$ was ruled out originally by Thas [26]. This result is a part of a more general theorem about the nonexistence of maximal arcs in $\mathrm{PG}(2, q)$ for odd q proved by Ball, Blokhuis and Mazzocca [4,5]. Since every $(2n + 2, 3)$-arc is extendable one gets that the size of an $(n, 3)$-arc is bounded by $n \leq 2q + 1$. This provides the best upper bound on the length of a near-MDS code (cf. Theorem 2(vi)).

Almost-MDS codes are equivalent to so-called n-tracks. An n-track is a set of points in $\mathrm{PG}(r, q)$ such that every r of them are in general position. Tables containing exact values and bounds on the maximal size of an n-track are contained in [3,8,9,20].

3 Near-MDS Codes over Small Fields

With no loss of generality, we consider only codes with $k \leq 2q$ and $n \geq 2k$. Near-MDS codes of dimension greater than $\frac{n}{2}$ are obtained as orthogonal to near-MDS codes with $k \leq \frac{n}{2}$.

In the binary case we can list all near-MDS codes. These are the extended Hamming $[8, 4, 4]$-code, the simplex $[7, 3, 4]$-code, the $[6, 3, 3]$-codes obtained by shortening the Hamming code of length 7, as well as, several trivial codes of dimensions one and two.

In the ternary case, we have one $[9, 3, 6]_3$-code associated with the affine plane $\mathrm{AG}(2, 3)$, one $[10, 4, 6]_3$-code, one $[11, 5, 6]_3$-code (the orthogonal to the Golay code) and one $[12, 6, 6]_3$-code (the extended ternary Golay code).

For codes over $\mathbb{F}_4$, there exist three non-isomorphic $[9, 3, 6]_4$-codes, associated with the three non-equivalent $(9, 3)$-arcs in $\mathrm{PG}(2, 4)$, two $[10, 4, 6]_4$-codes, exactly one $[11, 5, 6]_4$-code and exactly one $[12, 6, 6]_4$-code [12,13]. It should be noted that the $[12, 6, 6]_4$ was constructed by Dumer-Zinoviev in [15] as the first member of an infinite family of uniformly packed codes. Remarkably, this code yields a cascade representation of the extended binary Golay code.

There exist two non-isomorphic $[11, 3, 8]_5$ codes associated with the two $(11, 3)$-arcs in $\mathrm{PG}(2, 5)$. One of them extends to a $[12, 4, 8]_5$ code which cannot be further extended. A $[12, 6, 6]_5$-code does exist. It was constructed in [10] using a computer. Later on, Abatangelo and Larato [2] constructed six non-isomorphic codes with these parameters. They extended by two points the elliptic curve Γ_6 of degree 6 in $\mathrm{PG}(5, q)$ arising from a non-singular cubic curve of $\mathrm{PG}(2, q)$ via the canonical Veronese embedding

$$\nu : (X : Y : Z) \to (X^2 : XY : Y^2 : XZ : YZ : Z^2).$$

4 Near-MDS Codes of Maximal Length

Let us denote by $m'(k, q)$ the maximum possible length for which there exists a $[n, k]_q$ near-MDS code. The following theorem summarizes some straightforward observations about $m'(k, q)$.

Theorem 2. *Let k be a positive integer and let q be a prime power. Then*

(i) $m'(2, q) = 2q + 2$;
(ii) $m'(k, q) \leq m'(k - \alpha, q) + \alpha$, *for every* α *with* $0 \leq \alpha \leq k$;
(iii) $m'(k, q) = k + 1$ *for* $k > 2q$;
(iv) $m'(2q, q) = 2q + 2$;
(v) $m'(2q - 1, q) = 2q + 1$.
(vi) $m'(k, q) \leq 2q + k - 2$;

Near-MDS codes with parameters $[n, k]_q$ can be constructed from elliptic curves over $\mathbb{F}_q$ having exactly n rational points [27] (cf. also [1,2,17,18]). Such codes are referred to as elliptic codes. For every prime power $q = p^r$, p a prime, near-MDS codes exist for lengths up to $N_q(1)$, where $N_q(1)$ denotes the maximum number of $\mathbb{F}_q$-rational points an elliptic curve defined over $\mathbb{F}_q$ can have. By a result of Waterhouse [28], we know that for every $q = p^e$

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{for } p | \lceil 2\sqrt{q} \rceil \text{ and odd } e, \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases}$$

Due to extensive computational work by Bartoli, Marcugini, Milani and Pambianco [7,13,22,25], the exact values of $m'(k, q)$ were determined for all fields of order $q \leq 9$, as well as lower and upper bounds on the size of the longest near-MDS code for some larger fields. Even more results were obtained for the case of dimension three, which corresponds to the problem of the maximal size of an $(n, 3)$-arc in $\mathrm{PG}(2, q)$ (cf [21,23,24]). These results are summarized in the table below.

q/k	2	3	4	5	7	8	9	11	13	16
2	6	8	10	12	16	18	20	24	28	34
3	7	9	9	11	15	15	17	21	23	28
4	8	10	10	12	14	16	16	20-21	21-24	
5		11	11	11	13	15	16	18-22	21-25	
6		12	12	12	13	14	16	18-23	21-36	
7			9	11	14	15	17	18-24	21-27	
8			10	12	13	16	18	18-25	21-28	
9				11	13	14	19	19-26	21-29	
10				12	14	15	20	20-27	21-30	
11					14	15	16	18-28	21-31	
12					15	16	16	18-29	21-32	
13					15	15	16	18-30	21-33	
14					16	16	17	18-31	21-34	
15						17	17	18-32	21-35	
16						18	18	18-33	21-36	

5 An Upper Bound on the Maximal Length of a Near-MDS Code

According to Theorem 2(vi), we have $m'(k, q) \leq 2q + k - 2$. It can be seen from the table above that equality is achieved for several pairs (k, q). The following theorem gives an improvement over Theorem 2(vi) for sufficiently large dimensions.

Theorem 3. *There exist no* $[2q + k - 2, k]_q$ *near-MDS codes for* $k \geq q + 4$ *and* $q \geq 9$.

Proof. We are going to use the geometric interpretation of near-MDS codes. Fix an integer $q + 4 < k < q + \sqrt{q} + 3$. Let $\mathcal{K}$ be an arc with $2q + k - 2$ points in $\mathrm{PG}(k - 1, q)$, associated with a $[2q + k - 2, k]_q$ near-MDS code. Furthermore, let $P_1, \ldots, P_{k-2}$ be points from $\mathcal{K}$. By the properties of the arcs associated with near-MDS codes, these $k - 2$ points are in general position. Set

$$S = \langle P_1, P_2, \ldots, P_{k-2} \rangle,$$
$$S_i = \langle P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_{k-2} \rangle, \quad i = 1, \ldots, k - 2.$$

Obviously, $\dim S = k-3$, and $\dim S_i = k-4$. Let H be a hyperplane in $\mathrm{PG}(k-1,q)$ which does not contain any of the points $P_1,\ldots,P_{k-2}$.

At first, we are going to prove that there exists a point $Q \in S \cap H$ which is not contained in any of the subspaces S_i. Assume for a contradiction that such a point Q does not exist and the subspaces S_i cover all points of $S \cap H$. This means that the subspaces $S_i \cap H$ also cover all points of $S \cap H$. By duality, we get that there exist $k-2$ points in $\widetilde{S \cap H}$, the dual space to $S \cap H$, that block all hyperplanes. By the restriction on k, we have that $k-2 < q+\sqrt{q}+1$, and a well-known result of Heim [19] implies that this blocking set should contain a line. In other words, the subspaces S_i meet in a subspace of codimension 2 in S. This is a contradiction, because $\cap_{i=1}^{k-2} S_i = \varnothing$. This follows from the fact that the points $P_1,\ldots,P_{k-2}$ are in general position.

Now we can construct a plane π in H which does not meet any of the subspaces S_i. Fix a line L in H which is disjoint from $S \cap H$. The existence of such a line follows from the dimension formula. The plane $\pi = \langle L, Q\rangle$ meets S only in the point Q and is therefore disjoint from any subspaces S_i. Note that from the properties of the near-MDS codes and the arcs associated with them $|\mathcal{K}\cap\pi| \leq 3$.

Now consider a projections φ_i, $i=1,\ldots,k-2$, from each S_i to π given by

$$\varphi_i\colon \begin{cases} \mathcal{P}\setminus S_i \to \pi \\ P \qquad \to \langle S_i, P\rangle \cap \pi \end{cases},$$

where $\mathcal{P}$ is the set of points of $\mathrm{PG}(k-1,q)$. Obviously, all induced arcs $\mathcal{K}^{\varphi_i}$ are plane arcs with parameters $(2q+1,3)$.

If $P \in \mathcal{K}\cap\pi$, then P is contained in all induced arcs. Obviously $Q = S\cap\pi$ is also contained in all arcs $\mathcal{K}^{\varphi_i}$. Note that there are at most three such points. If R is a point from π which is contained neither in $\mathcal{K}$ nor in S, then it is contained in at most two of $\mathcal{K}^{\varphi_i}$ (since a hyperplane contains at most k points from $\mathcal{K}$). Counting the pairs $(P,\mathcal{K}^{\varphi_i})$ with $P \in \mathcal{K}^{\varphi_i}$ in two possible ways, we get

$$(k-2)(2q+1) \leq 2(q^2+q-3)+4(k-2),$$

whence $k \leq q+4$, a contradiction. Now it remains to use Theorem 2(ii) to obtain the nonexistence for all dimensions $k > q+4$.

Let us note that the proof of the nonexistence of $(2q+1,3)$-arcs would immediately imply the nonexistence of $[2q+k-2,k]_q$ near-MDS codes. All numerical evidence suggests that this is true for all $q \geq 8$, but no proof of the nonexistence of $(2q+1,3)$-arcs in $\mathrm{PG}(2,q)$ for large q seems to be known for the time being. There is a problem for $(n,3)$-arcs in $\mathrm{PG}(2,q)$ suggested by A. Blokhuis asking to determine a constant c such that $n/q < c < 2$ for q large enough, or a construction where $n/q > c > 1$ [6].

We finish with two conjectures for near-MDS codes that are similar to the famous Main Conjecture for MDS codes.

Weak Main Conjecture for NMDS codes. For all positive integers k and all prime powers q it holds that $m'(k,q) \leq 2(q+1)$.

Strong Main Conjecture for NMDS codes. There exists a universal constant c (not depending on q) such that $m'(k,q) \leq N_1(q) + c$.

Acknowledgments. This research has been supported by the Research Fund of Sofia University.

References

1. V. Abatangelo, B. Larato, Near-MDS codes arising from algebraic curves, *Discrete Math.* 301(1)(2005), 5–19.
2. V. Abatangelo, B. Larato, Elliptic near-MDS codes, *Designs, Codes and Cryptography.* 46(2008), 167–174.
3. T. I. Alderson, A. A. Bruen, Maximal AMDS Codes, *AAECC* 19(2) (2008), 87–98.
4. S. Ball, A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.* **126**(1998), 3377–3380.
5. S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of order q do not exist, *Combinatorica* **17**(1997), 31–47.
6. S. Ball, J. Hirschfeld, Bounds on (n,r)-arcs and their application to linear codes, *Finite Fields Appl.* **11**(2005), 326–336.
7. D. Bartoli, S. Marcugini, F. Pambianco, The non-existence of some NMDS codes and the extremal sizes of complete $(n,3)$-arcs in $PG(2,16)$, *Designs, Codes and Cryptography* **72**(1)(2014), 129–134.
8. M. de Boer, Almost MDS Codes, *Designs, Codes and Cryptography* **9**(2)(1996), 143–155.
9. M. de Boer, Codes: their parameters and Geometry, PhD Thesis, Eindhoven University of Technology, 1997.
10. I. Boukliev, J. Simonis, Some New Results on Optimal Codes over $\mathbb{F}_5$, *Designs, Codes and Cryptography* **30**(2003), 97–111.
11. S. Dodunekov, I. Landjev, On Near-MDS Codes, *J. Geometry* **54**(1995), 30–43.
12. S. Dodunekov, I. Landjev, On the quaternary $[11,6,5]$ and $[12,6,6]$ Codes, in: D. Gollmann (ed.) Applications of Finite Fields, IMA Conference Series 59, Clarendon Press, Oxford, 19996, 75–84.
13. S. Dodunekov, I. Landjev, Near-MDS Codes over Some Small Fields, *Discrete Math.* **213**(2000), 55–65.
14. S. Dodunekov, J. Simonis, Codes and projective multisets, *The Electronic Journal of Combinatorics*, **5**(1998), R37.
15. I. I. Dumer, V. A. Zinoviev, Some New Maximal Codes over GF(4), *Problemi Peredachi Informacii* **14**(1978), 24–34. (in Russian)

16. A. Faldum, W. Willems, Codes of Small Defect, *Designs, Codes and Cryptography* **10**(1997), 341–350.
17. M. Giulietti. On the extendability of Near-MDS elliptic codes. AAECC 15(1)(2004), 1-11.
18. M. Guilietti, F. Pasticci, On the completeness of certain n-tracks arising from elliptic curves, *Finite Fields and Appl.* 13(2007), 988–1000.
19. U. Heim, Blockierende Mengen in endlichen projecktiven Räumen, Litt. Math. Seminar Giessen, 1996, pp. 1–82. (also: Dissertation, Justus Liebig Universität Giessen, 1995.)
20. J.W.P. Hirschfeld, L.Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. Developments in Mathematics, vol.3, Kluwer Academic Publishers, Finite Geometries. Proc. Of the Fourth Isle of Thorns Conference (Chelwood Gate, July16-21,2000), Eds. A. Blokhuis. J.W.P. Hirschfeld, D. Jungnickel.,J.A. Thas), pp.201-246.
21. S. Marcugini, A. Milani, F. Pambianco, Maximal $(n,3)$-arcs in PG$(2,11)$, *Discrete Math.* **208/209**(1999), 421–426.
22. S. Marcugini, A. Milani, F. Pambianco. NMDS codes of maximal length over F_q, $8 \leq q \leq 11$. IEEE Trans. Inform. Theory, 48(4)(2002), 963-966.
23. S. Marcugini, A. Milani, F. Pambianco, Classification of the $(n,3)$-arcs in PG$(2,7)$, *J. Geometry* **80**(2004), 179-184.
24. S. Marcugini, A. Milani, F. Pambianco, Maximal $(n,3)$-arcs in PG$(2,13)$, *Discrete Math.* **294**(1999), 139–145.
25. S. Marcugini, A. Milani, F. Pambianco, Classification of linear codes exploting an invariant. *Contributions to discrete mathematics* 1(1), (2006),1-7.
26. J. A. Thas, Some results concerning $\{(q+1)(n-1);n\}$-arcs and $\{(q+1)(n-1)+1;n\}$-arcs in finite projective planes of order q, *J. Combin. Theory Ser. A* **19**(1975), 228–232.
27. M. A. Tsfasman, S. G. Vladut, Algebraic-Geometric Codes, Amsterdam, Kluwer, 1991.
28. W. G. Waterhouse, Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. **2**(1969), 521–560.