The Lengths of Projective Triply-Even Binary Codes

Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann

Abstract—It is shown that there does not exist a projective triply-even binary code of length 59. This settles the last open length for projective triply-even binary codes, which therefore exist precisely for the lengths 15, 16, 30, 31, 32, 45–51, and ≥ 60.

Index Terms—Divisible code, projective code, linear code, partial spread.

I. INTRODUCTION

DOUBLY-EVEN binary codes have been the subject of extensive research for decades. For recent applications and enumeration results we refer, e.g., to [1]. A substantial study has also been done for triply-even binary codes; see [2]. These two classes are special cases of so-called Δ-divisible codes, i.e., q-ary linear codes C with all (Hamming) weights divisible by an integer Δ > 1; see, e.g., [3].

Assuming that C has length n, dimension k and no all-zero coordinate, the columns of a k × n generator matrix of C span n (not necessarily distinct) one-dimensional subspaces of \( \mathbb{F}_q^k \) that can be viewed as points in the associated projective geometry, see e.g. [4] or [5, Chapter 17]. The codewords correspond to the hyperplanes of the geometry, and the weight of a codeword is the number or points outside of the corresponding hyperplane. This geometric setting provides a basis-free approach to linear codes (for details see the end of Section II). The Δ-divisibility of the linear code C translates into the following property of the associated multiset \( \mathcal{P} \) of points in \( \mathbb{F}_q^k \). For each hyperplane H of \( \mathbb{F}_q^k \) we have \( \#(\mathcal{P} \cap H) \equiv \#\mathcal{P} \mod \Delta \). In this case, we will say that the multiset \( \mathcal{P} \) is Δ-divisible, too.

For a general linear code C, the number of non-zero columns of a generator matrix of C is called the effective length of C. If the effective length equals the length, C is said to be of full length. The code C is called projective if it is full-length and any pair of columns of a generator matrix is linearly independent, i.e., if the associated multiset \( \mathcal{P} \) of points is actually a set.

Recently, Δ-divisible codes have been applied for obtaining upper bounds on the size of partial t-spreads in \( \mathbb{F}_q^k \), i.e., sets of t-dimensional subspaces in \( \mathbb{F}_q^k \) with pairwise trivial intersection, see e.g. [6], [7]. Due to the intersection property, every point of \( \mathbb{F}_q^k \) is covered by at most one element of a given partial t-spread. Calling every non-covered point a hole, the set of holes of a partial t-spread is \( q^{-t-1} \)-divisible; see, e.g., [6, Theorem 8], where also a generalization to so-called vector space partitions is considered.1 So, from the non-existence of \( q^{-t-1} \)-divisible sets of suitable size n (or equivalently, projective \( q^{-t-1} \)-divisible codes of effective length n), one can conclude the non-existence of partial t-spreads in \( \mathbb{F}_q^k \) of a certain cardinality. Indeed, all currently known upper bounds on the size of a partial t-spread can be obtained from such non-existence results for divisible codes; see, e.g., [6], [7].

Thus from an application point of view \( q^{-r} \)-divisible codes over \( \mathbb{F}_q \), where r is a positive integer (or, more generally, a positive rational number such that \( q^{-r} \) is an integer)2 are of considerable interest. If \( G_1 \) is a generator matrix of a Δ-divisible \( \{n_1, k_1\}_q \) code and \( G_2 \) is a generator matrix of another Δ-divisible \( \{n_2, k_2\}_q \) code, then \( \left( \begin{array}{c} G_1 \\ 0 \end{array} \right) \) is the generator matrix of a Δ-divisible \( \{n_1 + n_2, k_1 + k_2\}_q \) code. Since the set of all points of a k-dimensional subspace of \( \mathbb{F}_q^o \) is a \( q^{-k-1} \)-divisible point set in \( \mathbb{F}_q^o \) (where \( q \geq k \) can be any integer) and gcd((\( q^k - 1 \))/(\( q - 1 \)), (\( q^{k+1} - 1 \))/(\( q - 1 \)) = 1), for each prime power \( q \) and each \( r \in \mathbb{Q} \geq 0 \) such that \( q^r \in \mathbb{N} \), the set \( \mathcal{F}_q(r) \) of positive integers that do not occur as the cardinality of a \( q^{-r} \)-divisible (multi-)set or effective length of a (projective) \( q^{-r} \)-divisible code is actually a finite set (using a Frobenius Coin problem type argument for the proof). For multisets of points, i.e., not necessarily projective linear codes, the question is completely resolved: In [9, Theorem 4] for all integers \( r \) and all prime powers \( q \) the set \( \mathcal{F}_q(r) \) has been determined. For sets of points or projective \( q^{-r} \)-divisible codes the question is more complicated. A partial answer is given in [6, Theorem 13]:

\[
\text{Fact 1:} \quad (i) \quad 2^{1}-\text{divisible sets over } \mathbb{F}_2 \text{ of cardinality } n \text{ exist for all } n \geq 3 \text{ and do not exist for } n \in \{1, 2\}, \\
\quad (ii) \quad 2^{2}\text{-divisible sets over } \mathbb{F}_2 \text{ of cardinality } n \text{ exist for } n \in \{7, 8\} \text{ and all } n \geq 14, \text{ and do not exist in all other cases}, \\
\quad (iii) \quad 2^{3}\text{-divisible sets over } \mathbb{F}_2 \text{ of cardinality } n \text{ exist for } \\
\quad n \in \{15, 16, 30, 31, 32, 45, 46, 47, 48, 49, 50, 51\},
\]

1In a special case, the divisibility of the set of holes was already used in [8] to determine an upper bound for the maximum cardinality of a partial t-spread.

2cf. the beginning of Section II

Manuscript received December 15, 2018; revised July 5, 2019; accepted August 23, 2019. Date of publication September 13, 2019; date of current version April 21, 2020. T. Honold was supported by the National Natural Science Foundation of China under Grant 61571006.

T. Honold is with the ZJU-UIUC Institute, International Campus of Zhejiang University, Haining 314400, China (e-mail: honold@zju.edu.cn).

M. Kiermaier, S. Kurz, and A. Wassermann are with the Department of Mathematics, Physics, and Computer Science, University of Bayreuth, D-95447 Bayreuth, Germany (e-mail: michael.kiermaier@uni-bayreuth.de; sascha.kurz@uni-bayreuth.de; alfred.wassermann@uni-bayreuth.de).

Communicated by M. Schwartz, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2019.2940967
for all $n \geq 60$, and possibly for $n = 59$; in all other cases they do not exist.

In Part (iii) the existence question for a binary projective $2^4$-divisible code of length 59 remains undecided. The aim of this paper is to complete the characterization with the following theorem:

Theorem 2: There is no projective triply-even binary linear code of length 59.

Let us remark that the distinction between the existence of a projective/non-projective $q'$-divisible code of a certain length matters indeed, e.g., for the determination of upper bounds on the maximum possible cardinality of partial $t$-spreads. As an example, in [6, Theorem 13] (cf. also [7]) it is shown that no projective $2^3$-divisible code of length 52 exists, while there are non-projective examples with these parameters. From this non-existence result for projective $q'$-divisible codes we can conclude that there can be at most 132 solids in $\mathbb{F}_2^{11}$ with pairwise trivial intersection, which is the sharpest currently known upper bound. With a corresponding lower bound of 129, this is the smallest open case for the maximum cardinality of partial $t$-spreads over $\mathbb{F}_2$.

The remaining part of the paper is structured as follows. In Section II we state the necessary preliminaries from coding theory, before proving the non-existence of a binary projective $2^3$-divisible code of length $n = 59$ in Section III. In Section IV we derive a corollary which excludes the existence of vector space partitions of certain types. We close the paper with a discussion of some open problems in Section V.

II. Preliminaries

A linear code $C$ over $\mathbb{F}_q$ is called $q'$-divisible for some $r \in \mathbb{Q}_{>0}$ such that $q'^r \in \mathbb{N}$, if the weight of each codeword is divisible by $q'^r$. Given our assumption that $C$ is projective, the length equals the effective length, i.e., there are no zero-columns in the generator matrix of $C$, and $C$ corresponds to a set of $n$ points spanning $\mathbb{F}_q^k$. We denote the number of codewords of weight $i$ in $C$ by $a_i$ and the number of codewords of weight $i$ in the dual code $C^\perp$ by $a_i^\perp$. The well-known MacWilliams identities, see e.g. [11], relate the numbers $a_i$ and $a_i^\perp$ as follows. For all $i \in \{0, \ldots, n\}$ we have

$$\sum_{j=0}^{n} K_i(j)a_j = (\#C)a_i^\perp$$

for $i \in \{0, \ldots, n\}$,

where

$$K_i(j) = K_i^n,q(j) = \sum_{s=0}^{n} (-1)^{s}(q - 1)^{i-s}\binom{n-j}{i-s}\binom{j}{s}$$

is the $i$-th Kravchuk polynomial of order $n$. Obviously, we have $\sum_{i=0}^{n} a_i = \#C$, which is in fact the first ($i = 0$) MacWilliams equation. The polynomial $w(C) = \sum_{i=0}^{n} a_i x^i$ is called the weight enumerator of $C$.

3 More precisely, this conditions says that $q'^r$ should be an integral power of the field characteristic $p$. In [10, Theorem 1] it has been shown that $\Delta$-divisible codes with $\Delta$ relatively prime to $p$ correspond to repetitions of smaller codes. Thus, it suffices to consider the so-called modular case $\Delta = p^l$ for integers $l > 0$.

For a given $[n, k]_{q'}$ code $C$ and a codeword $c \in C$ of weight $w$ the residual code $C_c$ arises from $C$ by restricting all codewords to those coordinates where $c$ has a zero entry. Thus, $C_c$ is an $[n - w, \leq k - 1]_{q'}$ code. If $C$ is projective, then obviously also $C_c$ is projective. Moreover, if $C$ is $q'$-divisible, then $C_c$ is $q'^{-1}$-divisible; see, e.g., [6, Lemma 7].

It is well-known (see, e.g., [4]) that the relation $C \rightarrow C$, associating with a full-length linear $[n, k]$ code $C$ over $\mathbb{F}_q$ the $n$-multiset of $C$ of points in the projective geometry $PG(\mathbb{F}_q^k)$ defined by the columns of any generator matrix, induces a one-to-one correspondence between classes of (semi-)linearly equivalent full-length linear codes and classes of (semi-)linearly equivalent spanning multisets of points. The importance of the correspondence lies in the fact that it relates coding-theoretic properties of $C$ to geometric or combinatorial properties of $C$ via

$$w(aG) = n - \#\{1 \leq j \leq n; a \cdot g_j = 0\} = n - \#(C \cap a^\perp),$$

where $w$ denotes the Hamming weight, $G = (g_1 \ldots g_n) \in \mathbb{F}_q^{k \times n}$ a generating matrix of $C$, $a \cdot b = a_1 b_1 + \cdots + a_k b_k$, and $a^\perp$ is the hyperplane in $PG(\mathbb{F}_q^k)$ with equation $a_1 x_1 + \cdots + a_k x_k = 0$.4

In the usual coding theory setting, the Hamming weight depends on the chosen basis, as the standard basis vectors are exactly the vectors of Hamming weight 1. In contrast to that, the geometric setting provides a basis-free approach to linear codes.

III. Proof of the Main Theorem

In this section, we prove Theorem 2. For this purpose, let $C$ be a projective $8$-divisible binary code of length $59$ and minimum possible dimension $k$. We are going to restrict the weight frequencies $a_i$ in a series of lemmas, until we finally get a contradiction.

Lemma 1: $a_{48} = a_{56} = 0$.

Proof: The residual code of $C$ with respect to a codeword of weight $w$ is a projective $4$-divisible code of length $59 - w$. By Fact 1(ii), there is no such code of lengths $3$ or $11$. So the weights $w = 48$ and $w = 56$ are not possible.

Hence the only possible weights are $0, 8, 16, 24, 32$ and $40$. The first four MacWilliams identities give

$$(\begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 \\ 59 & 43 & 27 & 11 & -5 & -21 \\ 1711 & 895 & 335 & 31 & -17 & 191 \\ 32509 & 11997 & 2493 & -99 & 125 & -931 \end{array}) \begin{array}{c} a_0 \\ a_8 \\ a_{16} \\ a_{24} \\ a_{32} \\ a_{40} \end{array} = \begin{array}{c} a_1^\perp \\ a_2^\perp \\ a_3^\perp \\ a_4^\perp \end{array}.$$}

Of course, $a_0 = a_1^\perp = 1$. Since $C$ is projective, we have $a_1^\perp = a_2^\perp = 0$.

4In the non-projective case, $C \cap a^\perp$ must be interpreted as the multiset containing the points of $a^\perp$ with their $C$-multiplicities.
Multiplying the matrix of coefficients with the inverse of the rightmost $4 \times 4$ submatrix yields
\[
\begin{align*}
 a_{16} &= -10 - 4a_8 - \frac{45}{212} a_{12} \# C + \frac{1}{212} a_3 \# C, \\
 a_{24} &= 20 + 6a_8 + \frac{1447}{212} a_{12} \# C - \frac{3}{212} a_3 \# C, \\
 a_{32} &= -15 - 4a_8 + \frac{2617}{212} a_{12} \# C + \frac{3}{212} a_3 \# C, \\
 a_{40} &= 4 + a_8 + \frac{77}{212} a_{12} \# C - \frac{1}{212} a_3 \# C.
\end{align*}
\]

**Lemma 2:** $k \geq 10$.

**Proof:** $0 \leq a_{16} + a_{40} = -6 - 3a_8 + \frac{1}{128} \# C \leq -6 + \frac{1}{128} \# C$. Thus $2^k = \# C \geq 6 \cdot 128 = 768$. Therefore $k \geq 10$.

**Lemma 3:** $k = 10$.

**Proof:** Let $V = \mathbb{F}_2^8$ and $C$ the set of 59 points in $PG(V)$ corresponding to the linear code $C$.

Let $Q$ be a point in $PG(V)$ not contained in $C$. We consider the projection of $C$ modulo $Q$, that is the multiset image of $C$ under the map $V \rightarrow V/Q$, $v \mapsto (v + Q)/Q$. The resulting multiset $C'$ consists of $59$ points in $PG(V/Q) \cong PG(F_{2^5})$ and arises by identifying points of $C$ on the same line through $Q$. The corresponding linear code $C'$ is a subcode of $C$ of effective length $59$ and dimension $k - 1$. Therefore, $C'$ is $2_3$-divisible, and the assumed minimality of $k$ implies that $C'$ is not projective. Equivalently, there is a secant through $Q$, that is a line whose remaining two points are contained in $C$.

So each of the $2^k - 60$ points of $PG(V)$ not contained in $C$ lies on a secant. Since $C$ admits at most $\frac{\# C}{2^5} = \binom{59}{2} = 1711$ secants, covering at most $1711$ different points not in $C$, we get $2^k - 60 \leq 1711$ and therefore $k \leq 10$. Hence $k = 10$ by Lemma 2.

**Lemma 4:** $a_8 = 0$ and $a_{16} + a_{40} = 2$.

**Proof:** Plugging $\# C = 210$ from Lemma 3 into $a_{16} + a_{40} = -6 - 3a_8 + \frac{1}{128} \# C$ (proof of Lemma 2) yields $a_{16} + a_{40} = 2 - 3a_8$. As this expression cannot be negative, $a_8 = 0$ and $a_{16} + a_{40} = 2$.

**Lemma 5:** $a_{16} = 0$.

**Proof:** Assume that $a_{16} \neq 0$. Then by Lemma 4, either $(a_{16}, a_{40}) = (1,1)$ or $(a_{16}, a_{40}) = (2,0)$. Let $C$ be a codeword of weight $16$ and $\pi : C \rightarrow \mathbb{F}_2^5$ the restriction of $C$ to $supp(C)$, i.e., to the $16$ non-zero positions of $c$. Then $C' = \pi(C)$ is a $2_3$-binary code of effective length $16$. By the $2_3$-divisibility of $C$ and the fact that $C'$ contains the all-1-word, we see that $C'$ is $2_3$-divisible. Therefore, $C'$ is self-orthogonal of length $16$, implying that $dim(C') \leq \frac{16}{2} = 8$.

Assume that there exists a codeword $x \in \ker(\pi) \setminus \{0\}$. Then the supports of $x$ and $c$ are disjoint, so $w(x + c) = w(x) - 16$. In the case $(a_{16}, a_{40}) = (2,0)$ we have $w(x + c) \leq 32$, so $w(x) \leq 16$ and hence $x$ is uniquely determined as the other word of weight $16$. In the case $(a_{16}, a_{40}) = (1,1)$, $w(x) \geq 24$ (since the only word of weight $16$ is $c$). Hence $w(x) = 24$ and $w(x + c) = 40$. So $x + c$ is the unique codeword of weight $40$, and $x$ is uniquely determined as $(x + c) - c$.

Therefore in both cases $\dim ker(\pi) \leq 1$. The application of the rank-nullity theorem to $\pi$ then gives $dim C = dim ker(\pi) + dim im(\pi) \leq 1 + 8 = 9$, a contradiction.

**Lemma 6:** The code $C$ does not exist.

**Proof:** By Lemma 4 and 5, $a_{40} = 2$. Let $c$ be a codeword of weight $40$. We consider the restriction $\pi : C \rightarrow \mathbb{F}_2^{19}$ to the 0-coordinates of $c$. The image $D = \pi(C)$ is the residual code $C_e$, which is a binary projective $2_3$-divisible code of length $19$. The kernel $D' = ker \pi$ consists of all codewords of $C$ whose support is contained in $supp(c)$.

The first 5 MacWilliams equations for the residual code $D$ are
\[
\begin{pmatrix}
 1 & 1 & 1 & 1 & 1 \\
 19 & 11 & 3 & -5 & -13 \\
 171 & 51 & -5 & 3 & 75 \\
 969 & 121 & -23 & 25 & -247 \\
 3876 & 116 & 4 & -44 & 484
\end{pmatrix}
\begin{pmatrix}
 b_0 \\
 b_1 \\
 b_4 \\
 b_{12} \\
 b_{16}
\end{pmatrix}
= \# D \cdot
\begin{pmatrix}
 b_0^+ \\
 b_1^+ \\
 b_4^+ \\
 b_{12}^+ \\
 b_{16}^+
\end{pmatrix}.
\]

Using $b_0 = b_1^+ = 1$ and $b_4^+ = b_2^+ = 0$, the first 4 equations lead to
\[
\begin{pmatrix}
 b_0 \\
 b_1 \\
 b_4 \\
 b_{12} \\
 b_{16}
\end{pmatrix}
= \# D \cdot
\begin{pmatrix}
 15 + b_2^+ \\
 291 - 3b_3^+ \\
 205 + 3b_3^+ \\
 1 - b_3^+
\end{pmatrix} + \begin{pmatrix}
 -4 \\
 6 \\
 -4 \\
 1
\end{pmatrix}.
\]

Plugging these expressions into the fifth MacWilliams identity leads to
\[
b_4^+ = -11 - b_3^+ + \frac{12}{\# D}.
\]

Hence $0 \leq b_4^+ \leq -11 + \frac{12}{\# D}$, i.e., $\# D \leq \frac{12}{11} < 2^9$. Therefore, $\dim(D) \leq 8$.

The code $D'$ contains $c$. For $x \in D'$, $w(c + x) = 40 - w(x)$. So $D'$ cannot contain codewords of weights 8 or 16 (as $a_8 = a_{16} = 0$), nor of weight 24 or 32 (as $c + x$ would then have weight 16, resp., 8). Therefore, $D' = \{0, c\}$ and $\dim(D') = 1$. Application of the rank-nullity theorem to $\pi$ then yields $\dim(C) = \dim(D') + \dim(D) \leq 1 + 8 = 9$, the final contradiction.

**IV. APPLICATION TO VECTOR SPACE PARTITIONS**

Let $V$ be a finite vector space over $\mathbb{F}_q$. A set $P$ of non-zero subspaces of $V$ is called a vector space partition of $V$ if every non-zero vector of $V$ is contained in exactly one element of $P$. In other words, the elements of $P$ form a partition of the point set of $PG(V)$. Denoting the number of elements of dimension $i$ in $P$ by $d_i$, the type of $P$ is given by the sequence $(d_1, d_2, d_3, \ldots)$, or “multiplicatively” as $(1^{d_1} 2^{d_2} 3^{d_3} \ldots)$ with factors having $d_i = 0$ omitted.

**Corollary 3:** Let $V$ be a finite vector space over $\mathbb{F}_2$. There is no vector space partition of $V$ of type $(d_1)$ with $d_1 = 59$ and $d_2 = d_3 = 0$.

**Proof:** Assume that $P$ is a vector space partition of the given type. By [6, Theorem 8], the 59 subspaces of dimension 1 form an 8-divisible set of points in $PG(V)$. This set corresponds to a projective 8-divisible binary code of length 59, which does not exist by Theorem 2.

**Example 1:** The smallest nontrivial cases under Corollary 3 are vector space partitions of $\mathbb{F}_2^{10}$ of type $(1^{50} 4^{5} 5^{4})$ and of type $(1^{50} 4^{5} 5^{4} 7^{1})$.

\[\text{In fact, at this point the weight enumerator of } C \text{ is uniquely determined: } a_8 = a_{16} = 0 \text{ yields } a_3^+ = 85 \text{ and } w(C) = 1 + 318 x^{24} + 703 x^{32} + 2 x^{40}; \text{ cf. the proof of Lemma 2.}\]
V. Conclusion and Open Problems

Using purely theoretical methods we were able to exclude the existence of a projective $2^3$-divisible binary code of length 59. This completes the characterization of the possible lengths of projective $2^3$-divisible binary codes, which play some role in applications.

It would be desirable to have generalizations of the completed characterization in Fact 1 to other parameters. To this end, we state the list of lengths of projective $2^4$-divisible binary codes for which the existence question is undecided, at least according to our knowledge:

\{130, 163, 164, 165, 185, 215, 216, 232, 233, 244, 245, 246, 247, 274, 275, 277, 278, 306, 309\}.

For $q = 3$ the smallest open case is that of a projective $3^2$-divisible ternary code of length 70. The complete list of undecided lengths is

\{70, 77, 99, 100, 101, 102, 113, 114, 115, 128\}.

This paper is dedicated to Ivan Landjev on the occasion of his 59th birthday.

References

[1] C. F. Doran et al., “Codes and supersymmetry in one dimension,” Adv. Theor. Math. Phys., vol. 15, no. 6, pp. 1909–1970, 2011.
[2] K. Betsumiya and A. Munemasa, “On triply even binary codes,” J. London Math. Soc., vol. 86, no. 1, pp. 1–16, 2012.
[3] H. N. Ward, “An introduction to divisible codes,” Des., Codes Cryptogr., vol. 17, nos. 1–3, pp. 73–79, 1999.
[4] S. Dodunekov and I. Simonis, “Codes and projective multisets,” Electron. J. Combinatorics, vol. 5, no. 1, p. 37, 1998.
[5] J. Bierbrauer, Introduction to Coding Theory, London, U.K.: Chapman & Hall, 2004.
[6] T. Honold, M. Kiermaier, and S. Kurz, “Partial spreads and vector space partitions,” in Network Coding and Subspace Designs, M. Greferath, M. O. Pavčević, N. Silberstein, and M. Vázquez-Castro, Eds. Cham, Switzerland: Springer, 2018, pp. 131–170.
[7] S. Kurz, “Packing vector spaces into vector spaces,” Australas. J. Combinatorics, vol. 68, no. 1, pp. 122–130, 2017.
[8] A. Butlerspacher, “Partial spreads in finite projective spaces and partial designs,” Mathematische Zeitschrift, vol. 145, no. 3, pp. 211–229, 1975.
[9] M. Kiermaier and S. Kurz, “On the lengths of divisible codes,” Jul. 2017, arXiv:1707.00650. [Online]. Available: https://arxiv.org/abs/1707.00650
[10] H. N. Ward, “Divisible codes,” Archiv der Mathematik, vol. 36, no. 1, pp. 485–494, 1981.
[11] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes. Amsterdam, The Netherlands: Elsevier, 1977.

Thomas Honold received his academic qualifications (Diploma, Ph.D., and Habilitation) in Mathematics from TU Munich, Germany, in 1990, 1994, and 2000, respectively. He is currently working as professor for the ZJU-UIUC Institute at Zhejiang University’s International Campus in Haining, Zhejiang Province, China. Prior to this he has held positions at TU Munich (1993-2003, 2004/5, 2012), University of Eichstaett, Germany (2001), German Institute of Science and Technology, Singapore (2003/4), and Zhejiang University (2007-2017). His research interests include coding theory and geometry over finite fields and finite rings.

Michael Kiermaier received the Diploma degree in mathematics from the Technical University of Munich, Germany, in 2006 and the Ph.D. degree from the University of Bayreuth, Germany, in 2012. He is an assistant professor at the University of Bayreuth. His research interests include coding theory and geometry over finite fields and finite rings.

Sascha Kurz was born in Eschwege, Germany, in 1980. He received the Diploma degree and the Ph.D. degree in mathematics from the University of Bayreuth in 2004 and 2005, respectively. His research interest include network coding, the mathematics of voting systems, discrete optimization and discrete structures in general.

Alfred Wassermann received the Diploma degree 1988 and the Ph.D. degree 1992, both from the University of Bayreuth, Bayreuth, Germany. He received the Habilitation, also from the University of Bayreuth, in 2002. From 1989 until 1991 he held a Research Fellowship from Siemens ZFE, working in cryptography. Currently, he is an associate professor at the University of Bayreuth. His research interests include coding theory, random network coding, design theory and discrete optimization.