Erasure-Resilient Codes from Affine Spaces

Meinard Müller and Masakazu Jimbo

Keio University, Department of Mathematics, 3-14-1 Hiyoshi
Kohoku-ku, Yokohama 223-8522, Japan

Abstract

In this paper, we investigate erasure-resilient codes coming from Steiner 2-designs with block size k which can correct up to any k erasures. In view of applications it is desirable that such a code can also correct as many erasures of higher order as possible. Our main result is that the erasure-resilient code constructed from an affine space with block size q – a special Steiner 2-design – can not only correct up to any q erasures but even up to any $2q-1$ erasures except for a small set of so-called bad erasures if q is a power of some odd prime number. This gives a new family of erasure-resilient codes which is asymptotically optimal in view of the check bit overhead.

Key words: erasure-resilient codes, Steiner 2-designs, affine spaces

1 Introduction

To avoid high rates of data loss in large disk arrays, also known as redundant arrays of independent disks (RAID), Hellerstein et al. [4] introduced data redundancy in form of erasure-resilient codes to allow information to survive hardware failures. In view of this application, they point out that in a k-erasure-resilient code the fraction of sets of $k+1$ erasures that can be corrected has a significant effect on the overall reliablility of the code. However, in a k-erasure-resilient code with minimal update penalty it is impossible to correct any $(k+1)$-erasure consisting of an information bit and its k associated check bits, which is also referred to as *bad* erasure. Hence, in view of maximizing the reliability it is of interest to find k-erasure-resilient codes with minimal update penalty which can correct any $(k+1)$-erasure except for the bad ones. Among others, Hellerstein et al. [4] constructed a 3-erasure-resilient code based on a Steiner triple system which can correct any 4-erasure except for the bad ones.

Chee et al. [2] extended this concept by introducing the notion of (k, ℓ)-erasure-resilient codes, $k < \ell$. By definition, such codes are k-erasure-resilient codes which can correct up to any ℓ erasures except for the bad ones. In their paper, Chee et al. investigated (k, ℓ)-erasure-resilient codes from a set systems point of view, gave several constructions based on combinatorial designs and proved some upper and lower bounds concerning the asymptotical behaviour of the check bit overhead.

In this paper, we investigate erasure-resilient codes coming from Steiner 2-designs extending the results mentioned above of Hellerstein et al. [4]. Our main result is that affine spaces, which constitute a special class of Steiner 2-designs, over some ground field of odd order q lead to q-erasure-resilient codes which can correct up to any $2q-1$ erasures except for the bad ones (Theorem 4.2). This gives a new family of erasure-resilient codes which, as it turns out, satisfies the upper asymptotic bound concerning the check bit overhead given in the paper by Chee et. at. [2] and, hence, is optimal in this respect.

For some background information concerning the RAID-application and a detailed account on erasure-resilient codes we refer the reader to the literature [2–4]. In Section 2, we summarize the necessary coding theoretic background and introduce in Section 3 the codes coming from Steiner 2-designs. In Section 4, we prove our main result (Theorem 4.2), which is based on affine spaces over some ground field of odd order. We conclude this paper by proving that this construction does not work any longer when the ground field is of even order (Theorem 4.6). In this case there are actually $(q+1)$-erasures which are not bad.

2 Background from Coding Theory

In this section, we summarize the necessary facts from coding theory. Further details and references can be found in [2,4]. Let $m, c \in \mathbb{N}$ and let $\mathrm{GF}(2)$ denote the field with two elements. A *systematic binary linear* $(m+c, m)$*-code* is a linear injection $\gamma : \mathrm{GF}(2)^m \to \mathrm{GF}(2)^{m+c}$ such that an information $x \in \mathrm{GF}(2)^m$ appears unchanged in the first m bits – the so-called *information bits* – of the corresponding code vector $\gamma(x)$. The remaining c bits are referred to as *check bits* which can be computed as the parity of subsets of information bits. Each such code can be defined in terms of a $c \times (m+c)$*-control matrix* or *parity check matrix*, $H = [C|I]$, where I denotes the $c \times c$ identity matrix and C is a $c \times m$ matrix. The codewords in the code are the vectors $y \in \mathrm{GF}(2)^{m+c}$ satisfying the equation $Hy = 0$.

An unreadable bit of a codeword is called an *erasure*, i.e., an erasure is a defective bit or *error* where the position of this bit is known. It is a well known

fact that a code can *detect* up to any k errors, $k \in \mathbb{N}$, iff it can *correct* up to any k erasures. In terms of the parity check matrix H this is equivalent that any set of k columns from H are linearly independent considered as vectors over GF(2) (see [4]). A code with this property is called a *k-erasure-resilient code* and will be abbreviated as $[m, c, k]$-ERC or just k-ERC if the parameters m and c are not important in the context.

In view of the RAID-application one important metric in erasure-resilient codes is the *update penalty*. In terms of the matrix H it can be defined as the maximum over the weights of the colums of H. It follows easliy that the update penalty of an k-ERC is at least k. Hence, with respect to this metric, a k-ERC with parity check matrix $H = [C|I]$ is optimal if all columns of C have precisely weight k. From here on we consider only those k-ERC for which the the update penalty is k, i.e., the minimum possible. Note that in such codes it is impossible to correct the set of all $(k+1)$-erasures. In particular, because every information bit is associated with k check bits, it is impossible to correct the set of $(k+1)$-erasures consisting of an information bit and its k check bits. This leads to the following defintion.

Definition 2.1 *A t-erasure, $t \geq k+1$ is* bad *if it includes the failure of an information bit and all of its k associated check bits.*

In view of a high reliability of the code it is desirable that a k-ERC can correct as many ℓ-erasures, $\ell > k$, as possible. This leads to the following definition introduced in [2].

Definition 2.2 *Let $\ell \geq k$. An $[m, c, k, \ell]$-ERC is an $[m, c, k]$-ERC which can correct all t-erasures, for $k+1 \leq t \leq \ell$, except for the bad t-erasures.*

Again we write (k, ℓ)-ERC for $[m, c, k, \ell]$-ERC if the parameters m and c are not of importance. In terms of the parity-check matrix an (k, ℓ)-ERC can be characterized as in the following Lemma whose proof can be found in [2].

Lemma 2.3 *$H = [C|I]$ is the parity-check matrix of a (k, ℓ)-ERC if and only if for every t columns, $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_t$ of C, where $2 \leq t \leq \ell$, the vector $\boldsymbol{x} = \oplus_{i=1}^{t} \boldsymbol{c}_i$ has weight at least $\ell + 1 - t$.*

3 Erasure-Resilient Codes from Steiner 2-Designs

Erasure-resilient codes are closely related to combinatorial designs. To fix the notation we summarize the required facts from design theory and refer for further details to the standard literature such as [1]. In particular, we introduce Steiner 2-designs which are the basis for the erasure-resilient codes we are

interested in.

Let X be a finite set. A *set system* is a pair $(X, \mathcal{A})$, where $\mathcal{A} \subseteq 2^X$. The *order* of the set system is $|X|$. The elements of X are called *points* and the elements of $\mathcal{A}$ are called *blocks*. A set system $(X, \mathcal{A})$ is called k*-uniform* if for any block $A \in \mathcal{A}$, $|A| = k$ holds. The *replication number* of a point $x \in X$ is $r_x := |\{A \in \mathcal{A} | x \in A\}|$. The following definition will be used extensively throughout the rest of this paper.

Definition 3.1 *Let $(X, \mathcal{A})$ be a set system. A point $x \in X$ is called* odd (even) *if the replication number r_x is odd (even). With* $\mathrm{odd}(X, \mathcal{A})$ *we will denote the number of odd points in X.*

If the underlying set X is clear from the context, we will often speak of a set system $\mathcal{A}$ and write $\mathrm{odd}(\mathcal{A})$ instead of $\mathrm{odd}(X, \mathcal{A})$. With a given a parity-check matrix $H = [C|I]$ of an $[m, c, k]$-ERC one can associate a set system $(X, \mathcal{A})$, where $X = \{1, \ldots, c\}$, $|\mathcal{A}| = m$, and $\mathcal{A}$ contains precisely the supports of the columns of C as blocks. We also call $(X, \mathcal{A})$ the *set system of the erasure-resilient code* which is obviously k-uniform. In terms of set systems Lemma 2.3 can be reformulated as follows (see also [2]).

Lemma 3.2 *$(X, \mathcal{A})$ is the set system of a (k, ℓ)-ERC if and only if for every t blocks, $A_1, \ldots, A_t$ of $\mathcal{A}$, where $2 \leq t \leq \ell$, one has* $\mathrm{odd}(\{A_1, \ldots, A_t\}) \geq \ell + 1 - t$.

A k-uniform set system $(X, \mathcal{A})$ of order v is called a *Steiner 2-design*, denoted as $S(2, k; v)$, if every pair of distinct points of X is contained in exactly one block of $\mathcal{A}$. From such a Steiner 2-design one can obtain an erasure-resilient code with parity-check matrix $H = [C|I]$ by defining $C = (c_{i,j})$ to be the incidence matrix of $(X, \mathcal{A})$, i.e., if $X = \{x_1, \ldots, x_v\}$ and $\mathcal{A} = \{A_1, \ldots, A_b\}$, then $c_{i,j} = 1$ in case $x_i \in A_j$ and otherwise $c_{i,j} = 0$, $1 \leq i \leq v, 1 \leq j \leq b$. In the following, this code will be simply referred to as $S(2, k; v)$*-Steiner code*.

Lemma 3.3 *An $S(2, k; v)$-Steiner design is a $[b, v, k]$-ERC with $b = \frac{v(v-1)}{k(k-1)}$.*

Proof: Let $H = [C|I]$ be the parity check matrix of the Steiner code $(X, \mathcal{A})$. Since each block of $(X, \mathcal{A})$ consists of k points, every column of C has weight k. Furthermore, it is a well known fact from design theory that the number b of blocks of any $S(2, k; v)$ is as stated in the lemma (see [1]). Let $\mathcal{B} \subseteq \mathcal{A}$ denote a subset consisting of t blocks, $2 \leq t \leq k$. By definition, any pair of two distinct points is contained in exactly one block, i.e., two distinct blocks have at most one point in common. From this follows easily

$$\mathrm{odd}(\mathcal{B}) \geq t \cdot k - \sum_{i=1}^{t-1} 2i = t \cdot k - t \cdot (t-1) = t \cdot (k - t + 1) \geq k - t + 1.$$

Lemma 3.2 with $\ell = k$ finishes the proof. □

In general, Steiner codes are not $(k, k+1)$-ERC, i.e., there are uncorrectable $(k+1)$-erasures which are not bad. In the proof of Theorem 4.6 we will construct such examples. For a more special class of Steiner 2-designs, however, one has a much higher erasure-correcting capability as is shown in the next section.

4 Erasure-Resilient Codes from Affine Spaces

For any prime power q and natural number $n \geq 2$ there is the following well-known standard construction for Steiner 2-designs. Let $\mathrm{GF}(q)$ be the Galois field of order q. Define the set of points X to be an n-dimensional vector space over $\mathrm{GF}(q)$. Let $\mathcal{A}$ be the set of cosets of one-dimensional subspaces of X. In this case, the blocks are also called *lines*. Then one readily shows that $(X, \mathcal{A})$ is an $S(2, q; q^n)$ (see [1]). Coming from an *n-dimensional affine space* these Steiner 2-design, also denoted by $\mathrm{AG}_1(n, q)$, have nice "geometric" properties. Two lines of $\mathcal{A}$ are said to be *parallel* iff they are cosets of the same one-dimensional subspace of X. This defines an equivalence relation on $\mathcal{A}$, where each equivalence class forms a so-called *parallel class* containing each point of X exactly once. Furthermore, note that two lines of $\mathcal{A}$ intersect each other iff they lie in the same plane (coset of a two-dimensional subspace of X) and are non-parallel. To prove the main result (Theorem 4.2) of this paper the following lemma will be useful, which gives a lower bound on the number of odd points for certain subsystems of lines.

Lemma 4.1 *Let q be an odd prime power and let $\mathcal{B} = \{B_1, \ldots, B_t\}$, $t \geq 2$, be any subsystem of lines of the Steiner 2-design $\mathrm{AG}_1(2, q)$. Suppose there is a parallel class $\mathcal{P}$ of $\mathrm{AG}_1(2, q)$ such that $s := |\mathcal{B} \cap \mathcal{P}| < q$ and $t - s$ is odd. Then $\mathrm{odd}(\mathcal{B}) \geq q - s$. Furthermore, at least $q - s$ odd points of $\mathcal{B}$ lie on lines of $\mathcal{B} \setminus \mathcal{P}$.*

Proof: Let $\mathcal{B}$, $\mathcal{P}$, and s as postulated in the lemma. With a suitable enumeration we may assume $\mathcal{B} \cap \mathcal{P} = \{B_1, \ldots, B_s\}$. There are $q - s$ lines in $\mathcal{P} \setminus \mathcal{B}$. Fix any such line $P \in \mathcal{P} \setminus \mathcal{B}$. Note that any line B_i, $s+1 \leq i \leq t$, intersects P in exactly one point. Now, we proceed stepwise. Starting with the empty set we add in the ith step, $i = 1, \ldots, t$, the line B_i. Define a_i, $1 \leq i \leq t$, to be the number of odd points of $\{B_1, \ldots, B_i\}$ lying on P. Then, clearly $a_i = 0$ for $i = 1, \ldots, s$ and $a_{s+1} = 1$. In step i, $s+1 \leq i \leq t$, there are two possibilities:

- B_i intersects P in some odd point of $\{B_1, \ldots, B_{i-1}\}$. Then $a_i = a_{i-1} - 1$.
- B_i intersects P in some even point of $\{B_1, \ldots, B_{i-1}\}$. Then $a_i = a_{i-1} + 1$.

In any case $a_i + 1 \equiv a_{i-1} \bmod 2$. Therefore, since $a_{s+1} = 1$ and $t - s$ is odd by assumption, a_t is odd as well. In other words, there is an odd number of odd

points of $\mathcal{B}$ lying on P, in particular there is at least one such point. Since there are $q-s$ choices for $P \in \mathcal{P} \setminus \mathcal{B}$, the assertions of the lemma follow. $\square$

In an $\mathrm{AG}_1(n,q)$-Steiner code there are obviously non-bad $2q$-erasures which are not corrigible. For example, just take the subsystem consiting of $2q$ lines of two distinct parallel classes of $\mathrm{AG}_1(2,q)$ considered as a subspace of $\mathrm{AG}_1(n,q)$, where any point has clearly replication number two. Therefore, in view of erasure-correcting capability the next theorem gives the best possible result one may expect. It also generalizes a result of Hellerstein et al. [4], where the existence of an $S(2,3;3^n)$, $n \in \mathbb{N}$, which is an $(3,4)$-ERC is shown.

Theorem 4.2 *Let q be an odd prime power and $n \geq 2$ a natural number. Then the $\mathrm{AG}_1(n,q)$-Steiner code is an $[m,c,q,2q-1]$-ERC with $m = q^{n-1} \cdot \frac{q^n-1}{q-1}$ and $c = q^n$.*

Proof: The formulas for m and c follow from the definition of $\mathrm{AG}_1(n,q)$ and Lemma 3.3. In view of Lemma 3.2, we have to prove that for any set $\mathcal{B}$ of t lines of $\mathrm{AG}_1(n,q)$, where $2 \leq t \leq 2q-1$, one has $\mathrm{odd}(\mathcal{B}) \geq 2q-t$. Fix such a t and $\mathcal{B} = \{B_1, \ldots, B_t\}$ for the rest of the proof, which will be split up into three cases: Case 1: $n = 2, t$ odd, Case 2: $n = 2, t$ even, and Case 3: $n > 2$.

Case 1 ($n = 2, t$ odd): Since q is assumed to be an odd prime power $q+1$ is even. Since the number of parallel classes in $\mathrm{AG}_1(2,q)$ is $q+1$ and t is odd, there is at least one parallel class containing an even number of lines of $\mathcal{B}$. Under all such parallel classes containing an even number of lines of $\mathcal{B}$ pick a parallel class, call it $\mathcal{P}$, which is minimal with respect to this number, call it s. Then either $s = 0$ or all parallel classes contain at least one line of $\mathcal{B}$. Therefore, $s \leq \max\{0, t-q\}$ in any case. In the case when $2 \leq t < q$, we can argue as in the proof of Lemma 3.3 to get $\mathrm{odd}(\mathcal{B}) \geq t \cdot (q-t+1) \geq 2 \cdot (q-t) + t = 2q-t$. In the case when $t \geq q$, we can apply Lemma 4.1 (since $t-s$ is odd) to get $\mathrm{odd}(\mathcal{B}) \geq q - s \geq q - (t-q) = 2q-t$.

Case 2 ($n = 2, t$ even): We distinguish two cases. In the first case the number $|\mathcal{P} \cap \mathcal{B}|$ is even for any parallel class $\mathcal{P}$ of $\mathrm{AG}_1(2,q)$. Then we can partition the lines of $\mathcal{B}$ into $j = \frac{t}{2}$ pairs of lines, where each pair is contained in a parallel class. If $j = 1$, then $\mathrm{odd}(\mathcal{B}) = 2q \geq 2q-t$. If $j > 1$, then the four lines of any two of the j pairs have at most 4 intersection points. From this follows (just as in the proof of Lemma 3.3):

$$\begin{aligned} \mathrm{odd}(\mathcal{B}) &\geq j \cdot 2q - \sum_{i=1}^{j-1} 4i = 2(jq - j(j-1)) = j(2q - 2j + 2) \\ &\geq 2q - 2j + 2 \geq 2q - t, \end{aligned}$$

where we used $2q - 2j + 2 \geq 0$. In the second case there is at least one parallel class $\mathcal{P}$ of $\mathrm{AG}_1(2,q)$ such that $s := |\mathcal{P} \cap \mathcal{B}|$ is odd and therefore $t - s$ as

well. If $s \leq t-q$ we get $\mathrm{odd}(\mathcal{B}) \geq q-s \geq q-(t-q) = 2q-t$ applying Lemma 4.1 just as in Case 1. Now, suppose $s > t-q$. Each line of $\mathcal{B} \setminus \mathcal{P}$ intersects each line of $\mathcal{B} \cap \mathcal{P}$ in exactly one point. Therefore, there are at most $|\mathcal{B} \setminus \mathcal{P}| \cdot |\mathcal{B} \cap \mathcal{P}| = (t-s) \cdot s$ distinct intersection points of lines of $\mathcal{B}$ lying on some line of $\mathcal{B} \cap \mathcal{P}$. But then there are at least $s \cdot q - (t-s) \cdot s$ odd points of $\mathcal{B}$ lying on lines of $\mathcal{B} \cap \mathcal{P}$. Furthermore, since $t-s$ is odd, there are by Lemma 4.1 another $q-s$ odd points of $\mathcal{B}$ lying on lines of $\mathcal{B} \setminus \mathcal{P}$. Altogether, we get

$$\mathrm{odd}(\mathcal{B}) \geq s(q-t+s) + q - s \geq q - t + s + q - s = 2q - t,$$

where we used $q - t + s > 0$ and $s \geq 1$.

Case 3 ($n > 2$): In case all lines of $\mathcal{B}$ lie in a common plane, we may assume – by applying a suitable affine transformation – that this plane is just the one spanned by the first two coordinates. This reduces the problem to the case $n = 2$. In case $t = 2$, obviously $\mathrm{odd}(\mathcal{B}) \geq 2q - t$. Hence, we are left with the case where there are at least three lines of $\mathcal{B}$ not lying on a plane. We may assume that there are two lines, say B_1 and B_2, intersecting each other since otherwise trivially $\mathrm{odd}(\mathcal{B}) \geq 2q - t$. Let j, $2 \leq j \leq t-1$ be the number of lines in $\mathcal{B}$ lying on the plane P spanned by B_1 and B_2. Renumbering the lines of $\mathcal{B}$ we may assume that these lines are $B_1, \ldots, B_j$. We distinguish two cases. In the first case let $j > q$. Since B_t intersects P in at most one point, the set system $\{B_1, \ldots, B_j, B_t\}$ has at least $q-1$ odd points on $B_t \setminus P$. Any other line $B_i, j < i < t$ intersects B_t in at most one point, i.e., $\mathrm{odd}(\mathcal{B}) \geq (q-1) - (t-j-1) > 2q-t$. In the second case let $j \leq q$. Then $\mathrm{odd}(\{B_1, \ldots B_j\}) \geq j(q-j+1)$ which follows just as in the proof of Lemma 3.3. Furthermore, since any other line $B_i, j < i \leq t$ intersects P in at most one point, we get

$$\begin{aligned} \mathrm{odd}(\mathcal{B}) &\geq j(q-j+1) - (t-j) = -j^2 + j(q+2) - t \\ &= -(j-q)(j-2) + 2q - t \geq 2q - t, \end{aligned}$$

where we used $(j-q)(j-2) \leq 0$. □

This result is also of interest in view of the conjecture formulated by Chee et al. [2] concerning the asymptotic behaviour of the optimal check bit overhead for (k, ℓ)-ERC. We substantiate this statement.

Definition 4.3 *Given c, k, and ℓ, define $F(c, k, \ell)$ to be the maximum m such that there exists an $[m, c, k, \ell]$-ERC.*

In other words, $F(c, k, \ell)$ is the maximum number of information bits that can be supported by c check bits, if one desires an update penalty of k and wants to tolerate all t-erasures, $t \leq \ell$, except the bad ones. An $[m, c, k, \ell]$-ERC with $m = F(c, k, \ell)$ is said to have *optimal check bit overhead*. In [2] the following lower and upper bounds for $F(c, k, l)$ are given.

Theorem 4.4 *For any fixed k and ℓ such that $1 \leq k \leq \ell$, there exist positive constants a_1 and a_2 such that*

$$a_1 c^{(2k+1-\ell)/4} \leq F(c,k,\ell) \leq a_2 c^{k+1-\lfloor \ell/2 \rfloor},$$

for all positive integer c.

Chee et al. [2] speak out the conjecture that the upper bound describes the true asymptotic behaviour of $F(c,k,\ell)$. Theorem 4.2 verifies this conjecture for the case $k=q$, $\ell = 2q-1$ for odd prime powers q, as will be proved in the next corollary.

Corollary 4.5 *For an odd prime power q one has $F(c,q,2q-1) = \Theta(c^2)$. In particular, $F(c,q,2q-1) \geq \frac{1}{q^4} \cdot c^2$.*

Proof: From Theorem 4.4 one gets $F(c,q,2q-1) = O(c^2)$. For any $c > 0$ pick the $n \in \mathbb{N}$ such that $q^n \leq c < q^{n+1}$. By Theorem 4.2 there is an $[q^{n-1}, q^{n-1} \cdot \frac{q^n-1}{q-1}, q, 2q-1]$-ERC. Hence

$$F(c,q,2q-1) \geq q^{n-1} \cdot \tfrac{q^n-1}{q-1} \geq (q^{n-1})^2 = \tfrac{1}{q^4} \cdot (q^{n+1})^2 \geq \tfrac{1}{q^4} \cdot c^2.$$

□

We conclude this paper with the case where q is an even prime power.

Theorem 4.6 *If q is an even prime power and $n \geq 2$ then the $\mathrm{AG}_1(n,q)$-Steiner code is not a $(q, q+1)$-ERC. In particular, there is a set system $\mathcal{B}$ consisting of $q+1$ lines of $\mathrm{AG}_1(n,q)$ such that $\mathrm{odd}(\mathcal{B}) = 0$.*

Proof: Obviously, it suffices to prove the assertion for $n = 2$. Note that $1 = -1$ in $\mathrm{GF}(q)$ since q is an even prime power. Pick an arbitrary but fixed invertible element $\omega \in \mathrm{GF}(q) \setminus \{0\}$. We define the following $q+1$ distinct lines of $\mathrm{AG}_1(2,q)$:

$$\begin{aligned} B_\alpha &= \{\lambda \cdot (\omega + \alpha, \alpha) + (0,\alpha)\,,\ \lambda \in \mathrm{GF}(q)\},\ \ \alpha \in \mathrm{GF}(q), \\ B' &= \{\lambda \cdot (\omega, \omega) + (0,\omega)\,,\ \lambda \in \mathrm{GF}(q)\}, \end{aligned}$$

and $\mathcal{B} := \{B_\alpha | \alpha \in \mathrm{GF}(q)\} \cup \{B'\}$. We will show, that any two lines of $\mathcal{B}$ intersect in exactly one point and that all intersection points are different. This implies that there are $\frac{q(q+1)}{2}$ points in the set system $\mathcal{B}$ and any such point appears in exactly two lines of $\mathcal{B}$, i.e., $\mathrm{odd}(\mathcal{B}) = 0$ which proves the theorem.

For any $\alpha, \beta \in \mathrm{GF}(q), \alpha \neq \beta$, one has $\frac{\omega+\alpha}{\alpha} \neq \frac{\omega+\beta}{\beta}$ and $\frac{\omega+\alpha}{\alpha} \neq \frac{\omega}{\omega}$. In other words, any two lines of $\mathcal{B}$ are non-parallel and hence intersect in exactly one point. It is easily verified that

$$B_\alpha \cap B_\beta = \tfrac{1}{\omega}\left((\omega+\alpha)(\omega+\beta), \alpha\cdot\beta\right), \quad \alpha,\beta \in \mathrm{GF}(q), \alpha \neq \beta,$$
$$B_\alpha \cap B' = \tfrac{1}{\omega}\left((\omega+\alpha)^2, \alpha^2\right), \quad \alpha \in \mathrm{GF}(q).$$

Next, we show that the intersection points of different pairs of lines are different. Let $\alpha,\beta,\gamma,\delta \in \mathrm{GF}(q)$ with $\alpha \neq \beta, \delta \neq \gamma, \beta \neq 0$ and suppose $B_\alpha \cap B_\beta = B_\gamma \cap B_\delta$. From this one gets the two equations $(\omega+\alpha)(\omega+\beta) = (\omega+\gamma)(\omega+\delta)$ and $\alpha\cdot\beta = \gamma\cdot\delta$. If one plugs in $\alpha = \frac{\gamma\cdot\delta}{\beta}$ into the first equation and multiplies by β one gets $(\beta\omega+\gamma\delta)(\omega+\beta) = \beta(\omega+\gamma)(\omega+\delta)$. By another easy computation and dividing by ω one derives the equation $(\beta+\gamma)(\beta+\delta) = 0$, i.e., $\beta = \gamma$ or $\beta = \delta$. Since $\alpha = \frac{\gamma\cdot\delta}{\beta}$ one gets $\{\alpha,\beta\} = \{\gamma,\delta\}$. Similarly, one shows that $B_\alpha \cap B' = B_\beta \cap B'$ implies $\alpha = \beta$. Furthermore, from $B_\alpha \cap B_\beta = B_\gamma \cap B'$, $\alpha,\beta,\gamma \in \mathrm{GF}(q), \alpha \neq \beta$, one derives $\alpha = \beta$ which is not possible. □

References

[1] Beth, T., Jungnickel, D., Lenz, H.: Design Theory. Cambridge University Press, 1999.

[2] Chee, Y. M., Colbourn, C. J., Ling, A.: Asymptotically optimal erasure-resilient codes for large disk arrays. Discrete Applied Mathematics 102 (2000), 3–36.

[3] Chen, P., Lee, E., Gibson, G., Katz, R., Patterson, D.: RAID: High-performance, reliable secondary storage. ACM Computing Surveys 26 (1994), 145–185.

[4] Hellerstein, L., Gibson, G., Karp, R., Katz, R., Patterson, D.: Coding Techniques for Handling Failures in Large Disk Arrays. Algorithmica 12 (1994), 182–208.