Diskrete Mathematik und Optimierung

Steffen Hitzemann and Winfried Hochstättler:

On the Combinatorics of Galois Numbers

Technical Report feu-dmo012.08
Contact: steffen.hitzemann@arcor.de, winfried.hochstaettler@fernuni-hagen.de

FernUniversität in Hagen
Fakultät für Mathematik und Informatik
Lehrgebiet für Diskrete Mathematik und Optimierung
D – 58084 Hagen

2000 Mathematics Subject Classification: 05A10, 51D25
Keywords: interval decomposition, lattice of subspaces, Galois numbers

On the Combinatorics of Galois Numbers

Steffen Hitzemann
Karlsruhe Institute of Technology

Winfried Hochstättler
FernUniversität in Hagen

August 25, 2010

Abstract

We define interval decompositions of the lattice of subspaces of a finite-dimensional vector space. We show that such a decomposition exists if and only if there exists a family of linear forms with certain properties. As applications we prove that all finite-dimensional real vector spaces admit an interval decomposition, while $GF(2)^n$ has an interval decomposition if and only if $n \leq 4$. On the other hand, we present an interval decomposition of $GF(3)^5$. This partially answers a question of Faigle [4, 1].

1 Introduction

Goldman and Rota [2] defined the *Galois numbers* G_n^q as the total number of linear subspaces of $GF(q)^n$ and showed that they satisfy the recursion

$$\begin{aligned} & G_0^q = 1,\ G_1^q = 2. \\ G_n^q &= 2G_{n-1}^q + (q^{n-1} - 1)G_{n-2} \qquad \text{for } n \geq 2. \end{aligned}$$

Ulrich Faigle [4, 1] asked whether this has an immediate combinatorial interpretation in the following sense:

> Is it always possible to partition the lattice of subspaces of $GF(q)^n$ into two intervals of length $n-1$ and $(q^{n-1}-1)$ intervals of length $n-2$, for $n \geq 2$?

We consider such *interval decompositions* for vector spaces $\mathbb{F}^n$ of finite dimension over arbitrary fields $\mathbb{F}$ and show that the existence of such a decomposition is equivalent to the existence of what we call *pointwise irreflexive and antisymmetric linear forms* (Theorem 1). This immediately implies that for $n \geq 3$ an interval decomposition of $\mathbb{F}^n$ exists only if $\mathbb{F}^{n-1}$ admits an interval decomposition. We also show that $\mathbb{R}^n$ always has an interval decomposition.

Considering finite fields, we present an algorithm that, given all (canonical) interval decompositions of $GF(q)^{n-1}$, constructs all (canonical) interval decompositions of $GF(q)^n$ if they exist. This is used to show that $GF(2)^n$ has a unique (canonical) interval decomposition for $n \leq 4$ and has no such decomposition if $n \geq 5$. On the other hand, we present an interval decomposition of $GF(3)^5$ and report on an implementation of a special version of our algorithm that shows the existence of 52 such (canonical) decompositions with a certain structure.

The paper is organized as follows. In the next section we introduce the notation and prove the main results. In Section 3 we derive the algorithms, which are applied to $GF(2)$ and $GF(3)$ in the following section. We conclude with some remarks and open problems. Our notation should be fairly standard. If not explicitly defined otherwise, $\mathbb{F}$ will denote an arbitrary field, $\mathbb{F}^*$ denotes $\mathbb{F} \setminus \{0\}$, V denotes a vector space of finite dimension n over $\mathbb{F}$ with $n \geq 2$, and for a set $X \subseteq V$ we denote by $\langle X \rangle$ the linear closure of X. When $X = \{q\}$, we simply write $\langle q \rangle$ for $\langle X \rangle$.

2 The Main Theorem

2.1 Interval Decompositions

Definition 1. An *interval decomposition* of the lattice of subspaces of V is a triple (p_0, H_0, m), where

1. $p_0 \in V \setminus \{0\}$ is a *point*, i.e. it generates a one-dimensional subspace $U_0 = \langle p_0 \rangle$ of V.

2. H_0 is a subspace of co-dimension 1, i.e. a *hyperplane* of V such that $p_0 \notin H_0$, and

3. $m : Q \to \mathcal{H}$ is an injection from the set Q of one-dimensional subspaces, disjoint from U_0 and H_0 and represented by suitable points q, to the set $\mathcal{H}$ of hyperplanes different from H_0 that do not contain p_0, such that $q \in m(\langle q \rangle)$ for all $\langle < q \rangle \in Q$ and the intervals $[\langle q \rangle, m(\langle q \rangle)]$ in the lattice of subspaces of V are pairwise disjoint.

An interval decomposition is *proper*, if the map $m : Q \to \mathcal{H}$ is a bijection.

Example 1. Let $n = 2$, $p_0, h_0 \in V \setminus \{0\}$ and $m : V \setminus \{p_0, h_0\} \to V \setminus \{p_0, h_0\}$ the identity map. Clearly, (p_0, h_0, m) is a proper interval decomposition.

Proposition 1. *Given an interval decomposition (p_0, H_0, m), let $(p_i)_{i \in I}$ denote the generators of the one-dimensional subspaces of H_0, i.e. I is a suitable index set and each one-dimensional subspace of H_0 is generated by a p_i for a unique $i \in I$. Then $Q = \{\langle q_{i,\beta}\rangle \mid i \in I\}$, where $q_{i,\beta} := p_i + \beta p_0$ for $i \in I, \beta \in \mathbb{F}^*$.*

Proof. If $\lambda_0 p_0 + \lambda_i p_i + \lambda_j p_j = 0$, then $\lambda_0 p_0 = -(\lambda_i p_i + \lambda_j p_j) \in U_0 \cap H_0 = \{0\}$. Hence $\lambda_0 = 0$. Since p_i, p_j span different subspaces of H_0, we conclude that p_0, p_i, p_j are linearly independent for all $i \neq j \in I$.

Considering $0 = \lambda(p_i + \beta p_0) + \mu(p_j + \beta' p_0) = \lambda p_i + \mu p_j + (\lambda\beta + \mu\beta')p_0$ and the above, we find that $p_i + \beta p_0$ and $p_j + \beta' p_0$ are linearly independent if either $i \neq j$ or $\beta \neq \beta'$.

Clearly, $p_i + \beta p_0$ is not a multiple of p_0. Assuming $p_i + \beta p_0 \in H_0$ yields the contradiction $\beta^{-1}(p_i + \beta p_0 - p_i) = p_0 \in H_0$. We conclude that for all $i \in I$ and $\beta \in \mathbb{F}^*$ the subspace $\langle p_i + \beta p_0\rangle$ lies neither in the filter generated by U_0 in the lattice of subspaces of V nor in the ideal of H_0. Hence the points $p_i + \beta p_0$ generate pairwise different one-dimensional subspaces that are disjoint from p_0 and H_0. Let $q_{i,\beta} = p_i + \beta p_0$.

On the other hand suppose that q generates such a one-dimensional subspace of V. By the rank formula of linear algebra, there exists a nonzero point $p \in H_0$, expressible as $p = \alpha_1 p_0 + \alpha_2 q$. Clearly, α_1 and α_2 must be nonzero. Hence $q = \alpha_2^{-1} p + \alpha_2^{-1}(-\alpha_1)p_0$. We conclude that there exists some nonzero element $\gamma \in \mathbb{F}$ and some $i \in I$ such that $q = \gamma q_{i,\beta}$. Thus, we have $Q = \{\langle q_{i,\beta}\rangle \mid i \in I\}$. □

2.2 Pointwise irreflexive and antisymmetric linear forms

Given an interval decomposition (p_0, H_0, m), for $i \in I$, $\beta \in \mathbb{F}^*$ and $q_{i,\beta} = p_i + \beta p_0$, we denote $m(\langle q_{i,\beta}\rangle)$ by $H_{i,\beta}$. The hyperplane $H_{i,\beta}$ is the kernel of the linear form $\sigma_{i,\beta} : V \to \mathbb{F}$ defined by

$$\sigma_{i,\beta}(p) := \begin{cases} 0 & \text{if } p \in H_{i,\beta} \cap H_0 \\ 0 & \text{if } p = p_i + \beta p_0 \\ \beta & \text{if } p = p_i. \end{cases} \tag{1}$$

Lemma 1. *If $p_j \in H_0$, then*

$$p_j + \beta' p_0 \in H_{i,\beta} \iff \sigma_{i,\beta}(p_j) = \beta'.$$

Proof. By definition $\sigma_{i,\beta}(p_0) = -1$, and hence

$$\sigma_{i,\beta}(p_j + \beta' p_0) = \sigma_{i,\beta}(p_j) - \beta'.$$

□

Definition 2. Let H_0 be a hyperplane of V. Denote a set of generators of the points of H_0 by $\{p_i \mid i \in I\}$. Let S be a set of linear forms indexed by I and $\mathbb{F}^*$, with

$$S = \{\sigma_{i,\beta} : V \to \mathbb{F} \mid i \in I, \beta \in \mathbb{F}^*\}.$$

We say that S is *pointwise irreflexive and antisymmetric on* H_0, if $\sigma_{i,\beta}(p_i) = \beta$ for $i \in I$ and

$$\sigma_{j,\beta'}(p_i) = \beta \Rightarrow \sigma_{i,\beta}(p_j) \neq \beta'$$

for distinct $i, j \in I$.

Example 2. Let V be the finite-dimensional vector space $\mathbb{R}^n$ with Euclidean norm $\|\cdot\|_2$. Let e_0 be a unit vector and $H_0 = e_0^\perp$ its orthogonal complement. As generators for the one-dimensional subspaces of H_0, we choose those $p_i \in H_0$ such that $\|p_i\| = 1$ and the first non-zero coordinate is positive. For such a $p \in \{p_i\}$ and $\beta \in \mathbb{R}^*$, we define $\sigma_{p,\beta} : V \to \mathbb{F}$ by

$$\sigma_{p,\beta}(s) = (-e_0^\top + \beta p^\top)s. \tag{2}$$

These linear forms are irreflexive, since for p as above we have

$$\sigma_{p,\beta}(p) = \beta\|p\|^2 = \beta.$$

Now let $p' \in H_0$ be another vector of unit length where the first non-zero coordinate is positive, and assume that

$$\beta'(p'^\top p) = \sigma_{p',\beta'}(p) = \beta.$$

Now $\sigma_{p,\beta}(p') = \beta p^\top p' = \beta'(p^\top p')^2$. Hence $\sigma_{p,\beta}(p') = \beta' \Rightarrow (p^\top p')^2 = 1$. By the Cauchy-Schwarz Inequality, this implies $p = \pm p'$. Since both are vectors of unit length where the first non-zero coordinate is positive, we necessarily have $p = p'$ and $\beta = \beta'$. Hence the linear forms are also pointwise antisymmetric.

The construction in (2) generalizes to complex vector spaces with Hermitian inner product.

Proposition 2. *Let $H_0, p_i, i \in I$ and S be as in Definition 2. Let $W \not\subseteq H_0$ be a subspace of V of dimension at least 2. If $H_0^W = H_0 \cap W$, and $I^W = \{i \in I \mid p_i \in H_0^W\}$, and $S^W = \{(\sigma_{i,\beta})_{|W} : W \to \mathbb{F} \mid i \in I^W, \beta \in \mathbb{F}^*\}$, then S^W is pointwise irreflexive and antisymmetric on H_0^W.*

Proof. The points p_i for $i \in I^W$ form a set of generators of the points of H_0^W, and the validity of the other two axioms is inherited. □

2.3 The equivalence

Theorem 1. *If $p_0 \in V \setminus \{0\}$, and H_0 is a hyperplane of V not containing $\langle p_0 \rangle$, then there exists an injection $m : Q \to \mathcal{H}$ such that (p_0, H_0, m) is an interval decomposition of the lattice of subspaces of V if and only if there exists a set $\{\sigma_{i,\beta} : V \to \mathbb{F} \mid i \in I, \beta \in \mathbb{F}^*\}$ of linear forms that is pointwise irreflexive and antisymmetric on H_0.*

Proof. First assume there is an interval decomposition and define $S = \{\sigma_{i,\beta}\}_{i,\beta}$ as in (1). By definition $\sigma_{i,\beta}(p_i) = \beta$. To verify the second condition suppose to the contrary that for some distinct $i, j \in I$

$$\sigma_{j,\beta'}(p_i) = \beta \text{ and } \sigma_{i,\beta}(p_j) = \beta'.$$

By Lemma 1 we have $p_i + \beta p_0 \in H_{j,\beta'}$ as well as $p_j + \beta' p_0 \in H_{i,\beta}$. Hence

$$\langle \{p_i + \beta p_0, p_j + \beta' p_0\} \rangle \in [p_i + \beta p_0, H_{i,\beta}] \cap [p_j + \beta' p_0, H_{j,\beta'}],$$

contradicting the properties of an interval decomposition.

Now assume that a pointwise irreflexive and antisymmetric set of linear forms is given and define

$$H_{i,\beta} = m(p_i + \beta p_0) := \langle \{p_i + \beta p_0\} \cup (H_0 \cap \ker(\sigma_{i,\beta})) \rangle. \tag{3}$$

Define $\tilde{\sigma}_{i,\beta}$ with respect to $H_{i,\beta}$ by (1) and note that $\tilde{\sigma}_{i,\beta}$ and $\sigma_{i,\beta}$ coincide on H_0. Hence $\{\tilde{\sigma}_{i,\beta} : V \to \mathbb{F} \mid i \in I, \beta \in \mathbb{F}^*\}$ is another family of linear forms that is pointwise irreflexive and antisymmetric on H_0; call this family $\tilde{S}$.

We now show that (p_0, H_0, m) is an interval decomposition. Clearly, none of the $p_i + \beta p_0$ is contained in H_0. The assumption $p_0 \in H_{i,\beta}$ yields $p_0 = \lambda(p_i + \beta p_0) + z$ for some $0 \neq z \in H_0 \cap \ker(\sigma_{i,\beta})$ and thus the contradiction $p_0 \in H_0$. (Note that $\lambda p_i \notin \ker(\sigma_{i,\beta}) \ni z$).

Hence it suffices to verify

$$[p_i + \beta p_0, H_{i,\beta}] \cap [p_j + \beta' p_0, H_{j,\beta'}] = \emptyset$$

for all $(i, \beta) \neq (j, \beta')$. Suppose to the contrary there exists

$$W \in [p_i + \beta p_0, H_{i,\beta}] \cap [p_j + \beta' p_0, H_{j,\beta'}].$$

We conclude that $p_i + p_j + (\beta + \beta')p_0 \in W$. Since $p_0 \notin W$, there exists some $k \in I, \lambda \in \mathbb{F}^*$ such that $\lambda p_k = p_i + p_j$, and Lemma 1 implies that $\tilde{\sigma}_{i,\beta}(p_k) = \lambda^{-1}(\beta + \beta') = \tilde{\sigma}_{j,\beta'}(p_k)$. Since $\tilde{\sigma}_{i,\beta}(p_k) = \lambda^{-1}(\tilde{\sigma}_{i,\beta}(p_i) + \tilde{\sigma}_{i,\beta}(p_j))$ and $\tilde{\sigma}_{i,\beta}(p_i) = \beta$, we conclude that $\tilde{\sigma}_{i,\beta}(p_j) = \beta'$. By symmetry we also have $\tilde{\sigma}_{j,\beta'}(p_i) = \beta$, contradicting $\tilde{S}$ being pointwise irreflexive and antisymmetric on H_0. $\square$

Remark 1. *If the definition in (3) makes m a bijection, then the interval decomposition is proper. This in particular holds, if $\mathbb{F}$ is finite or $\mathbb{F} = \mathbb{R}$ and $\sigma_{i,\beta}$ is given as in (2).*

Theorem 1 and Proposition 2 imply:

Corollary 1. *If $\mathbb{F}^n$ has an interval decomposition, then also $\mathbb{F}^k$ has an interval decomposition for all $2 \leq k \leq n$.*

And Example 2 yields

Corollary 2. *If $n \geq 2$, then $\mathbb{R}^n$ has an interval decomposition.*

Remark 2. *We may view the linear forms in Definition 2 as linear forms defined only on H_0, since their value outside of H_0 does not matter.*

We conclude this section by showing that a proper interval decomposition yields a partition of the lattice of subspaces.

Theorem 2. *Let (p_0, H_0, m) be a proper interval decomposition, and let $W \subseteq V$ be a subspace of V. Either $p_0 \in W$, or $W \subseteq H_0$, or there exists $\langle q \rangle \in Q$ such that $q \in W \subseteq m(\langle q \rangle)$.*

Proof. We proceed by induction on the dimension n of V. If $n = 2$, then the assertion is immediate. Thus assume $n > 2$. We may assume that neither $p_0 \in W$, nor $W \subseteq H_0$. If $\dim(W) = n - 1$, then $W \in m(Q)$, since the interval decomposition is proper, and we are done. Otherwise, let H' be a hyperplane of V containing H' and let $I^{H'}$, $S^{H'}$ be as in Proposition 2. By the induction hypothesis there exist some $i \in I^{H'}$ and $\beta \in \mathbb{F}^*$ such that $W \in [q_{i,\beta}, \langle \{q_{i,\beta}\} \cup (\ker((\sigma_{i,\beta})_{|H'}) \cap H_0 \cap H')\rangle]$. Hence $q_{i,\beta} \in W \subseteq m(\langle q_{i,\beta} \rangle)$. □

3 Algorithms

Theorem 1 and Proposition 2 enable us to derive an algorithm to compute interval decompositions, if they exist, by computing a set of irreflexive and antisymmetric linear forms from the corresponding forms for the projections. It will be helpful to choose a basis $\{b_1, \ldots, b_{n-1}\}$ of H_0 such that the matrix $(\sigma_{b_i,1}(b_j))_{i,j}$ is lower triangular.

Definition 3. Let $S = \{\sigma_{i,\beta} : V \to \mathbb{F} \mid i \in I, \beta \in \mathbb{F}^*\}$ be a set of linear forms that is pointwise irreflexive and antisymmetric on H_0 and $(b_1, \ldots, b_{n-1})$ an ordered basis of H_0. We say that S is *in canonical form with respect to* $(b_1, \ldots, b_{n-1})$ if

$$\forall 1 \leq i < k \leq n - 1 : \sigma_{b_i,1}(b_k) = 0.$$

Proposition 3. *If $S = \{\sigma_{i,\beta} : V \to \mathbb{F} \mid i \in I, \beta \in \mathbb{F}^*\}$ is a set of linear forms that is pointwise irreflexive and antisymmetric on H_0, then there exists an ordered basis $(b_1, \ldots, b_{n-1})$ of H_0 such that S is in canonical form with respect to $(b_1, \ldots, b_{n-1})$.*

Proof. Choose p_{i_0}, $i_0 \in I$ arbitrarily but fixed, and set $b_1 = p_{i_0}$. For $2 \le j \le n-1$, choose

$$b_j \in H_0 \cap \bigcap_{k=1}^{j-1} \ker(\sigma_{b_k,1}) \setminus \{0\}.$$

Such a choice is always possible since

$$\dim \left(H_0 \cap \bigcap_{j=1}^{i-1} \ker(\sigma_{b_j,1}) \right) \ge n - i.$$

Using $\sigma_{b_j,1}(b_j) = 1$ and the above choice, it is easy to show that the $b_1, \ldots b_{n-1}$ are linearly independent and hence form a basis of H_0. □

Note that $(p_0, b_1, \ldots, b_{n-1})$ is an ordered basis of V. The following is also immediate:

Proposition 4. *Let S be in canonical form with respect to $(b_1, \ldots, b_{n-1})$, and let $H_i = \langle \{p_0, b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{n-1}\} \rangle$. Then S^{H_i} is in canonical form with respect to $(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_{n-1})$.*

From now on we assume that $\mathbb{F}$ is a finite field. We may assume that $(p_0, b_1, \ldots, b_{n-1})$ is an ordered basis of $\mathbb{F}^n$. If we know the set $\tilde{\mathcal{S}}$ of all possible sets of irreflexive and antisymmetric linear forms $\tilde{S}$ on a hyperplane $\tilde{H}_0$ of $\mathbb{F}^{n-1}$ that are in canonical form with respect to a certain basis, then considering the projections of such linear forms for $\mathbb{F}^n$ on the H^i for $i = 1, \ldots, n$ as in the above proposition will yield an element of $\tilde{\mathcal{S}}^{n-1}$.

We examine each of these $(n-1)$-tuples to test whether it "generates" a suitable set of linear forms for $\mathbb{F}^n$. Given such a tuple $(S_1, \ldots, S_{n-1})$, we first check for all $i \neq j$ whether $S_{i|H_i \cap H_j} = S_{j|H_i \cap H_j}$. We then construct a suitable S and check whether it is pointwise irreflexive and antisymmetric.

We will demonstrate this algorithm in the next section and apply it in the case $\mathbb{F} = GF(2)$. Before doing so, we will introduce more structure into our linear forms to reduce the computational effort in our search for the case $|\mathbb{F}| > 2$.

Definition 4. Let $\{\sigma_{i,\beta} : V \to \mathbb{F} \mid i \in I, \beta \in \mathbb{F}^*\}$ be a set of linear forms that is pointwise irreflexive and antisymmetric on H_0. Denote this set by S. We call S *structured* if for all $i \in I$ and all $\beta, \beta' \in \mathbb{F}^*$ we have

$$\ker(\sigma_{i,\beta}) \cap H_0 = \ker(\sigma_{i,\beta'}) \cap H_0.$$

Such a structured set of linear forms may be considered as a one-to-one correspondence between the points and hyperplanes of H_0. Also note that in the case of $\mathbb{F} = GF(2)$ any set of irreflexive and antisymmetric linear forms is structured. The same holds for the linear forms in Example 2.

The following is again immediate:

Proposition 5. *A projection of a structured set of irreflexive and antisymmetric linear forms is structured.*

Thus, in our above algorithm we may restrict our search to structured sets of linear forms. We will report on an implementation of this method for $\mathbb{F} = GF(3)$ in the following section.

4 $GF(2)$ and $GF(3)$

4.1 GF(2)

Since $GF(2)^*$ has only one element, we omit the subscript β in this subsection. For $n = 2$ there is only one non-zero linear form $\sigma_{b_1} : H_0 \to GF(2)$. If $n = 3$, let $\{b_1, b_2\}$ be a basis of H_0, and let (d_0, d_1, d_2) be the ordered basis of linear forms dual to (p_0, b_1, b_2). Considering only linear forms that are in canonical form with respect to (p_0, b_1, b_2), irreflexivity implies $\sigma_{b_1} = d_1$. Now, irreflexivity and antisymmetry yield $\sigma_{b_1+b_2} = d_2$ and, finally, $\sigma_{b_2} = d_1 + d_2$.

Now, let $n = 4$, and (d_0, d_1, d_2, d_3) be the basis dual to (p_0, b_1, b_2, b_3). Considering the projections on H_3, H_2, H_1 and using the property of the canonical form, we find that

$$\sigma_{b_1} = d_1,\ \sigma_{b_2} = d_1 + d_2,\ \sigma_{b_1+b_2} = d_2 + \alpha_1 d_3,\ \sigma_{b_3} = d_1 + \beta_1 d_2 + d_3,$$
$$\sigma_{b_1+b_3} = \beta_2 d_2 + d_3,\ \sigma_{b_3} = \gamma_1 d_1 + d_2 + d_3, \sigma_{b_2+b_3} = \gamma_2 d_1 + d_3.$$

To make this compatible we have to set $\beta_1 = \gamma_1 = 1$. Hence $\sigma_{b_3} = d_1+d_2+d_3$. Irreflexivity allows for $\sigma_{b_1+b_2+b_3}$ only the choices d_i for $i \in \{1, 2, 3\}$ or $d_1 + d_2 + d_3$. By antisymmetry we are left with $\sigma_{b_1+b_2+b_3} = d_2$ or $\sigma_{b_1+b_2+b_3} = d_3$. Assuming the latter, we find that

$$\sigma_{b_1+b_2+b_3}(b_3) = 1 = \sigma_{b_3}(b_1 + b_2 + b_3),$$

contradicting antisymmetry. Hence we are left with $\sigma_{b_1+b_2+b_3} = d_2$ and conclude that $\alpha_1 = 1, \beta_2 = 0$ and $\gamma_2 = 1$. Altogether, we have

b_1	b_2	$b_1 + b_2$	b_3	$b_1 + b_3$	$b_2 + b_3$	$b_1 + b_2 + b_3$
d_1	$d_1 + d_2$	$d_2 + d_3$	$d_1 + d_2 + d_3$	d_3	$d_1 + d_3$	d_2

and verify that this set of linear forms is indeed irreflexive and antisymmetric on H_0. Summarizing, we find:

Proposition 6. *For $n \in \{2, 3, 4\}$ there exists one unique set of linear forms that is irreflexive and antisymmetric on H_0 and in canonical form with respect to $(p_0, b_1), (p_0, b_1, b_2)$, or (p_0, b_1, b_2, b_3), respectively.*

The existence of an interval decomposition for $GF(2)^n$ for $n \in \{2, 3, 4\}$ was proved by a different method in [4].

In the following we will show that there is no interval decomposition of $GF(2)^5$. Suppose to the contrary there were such an interval decomposition (p_0, H_0, m), and assume it were in canonical form with respect to an ordered basis (b_1, b_2, b_3, b_4) of H_0. Define H_4, H_3, H_2 and H_1 as in Proposition 4. Then the projection of (p_0, H_0, m) on each of the H_i is unique, by Proposition 6, and in canonal form, by Proposition 4. Thus, using a similar approach as in the case $n = 4$, we derive the following table:

b_1	b_2	$b_1 + b_2$	b_3
d_1	$d_1 + d_2$	$d_2 + d_3 + \alpha_1 d_4$	$d_1 + d_2 + d_3$
$b_1 + b_3$	$b_2 + b_3$	$b_1 + b_2 + b_3$	$b_1 + b_2$
$d_3 + \alpha_2 d_4$	$d_1 + d_3 + \alpha_3 d_4$	$d_2 + \alpha_4 d_4$	$d_2 + \beta_1 d_3 + d_4$
b_4	$b_1 + b_4$	$b_2 + b_4$	$b_1 + b_2 + b_4$
$d_1 + d_2 + \beta_2 d_3 + d_4$	$\beta_3 d_3 + d_4$	$d_1 + \beta_4 d_3 + d_4$	$d_2 + \beta_5 d_3$
$b_1 + b_3$	b_4	$b_1 + b_4$	$b_3 + b_4$
$\gamma_1 d_2 + d_3 + d_4$	$d_1 + \gamma_2 d_2 + d_3 + d_4$	$\gamma_3 d_2 + d_4$	$d_1 + \gamma_4 d_2 + d_4$
$b_1 + b_3 + d_4$	$b_2 + b_3$	b_4	$b_2 + b_4$
$\gamma_5 d_2 + d_3$	$\delta_1 d_1 + d_3 + d_4$	$\delta_2 d_1 + d_2 + d_3 + d_4$	$\delta_3 d_1 + d_4$
$b_3 + b_4$	$b_2 + b_3 + b_4$		
$\delta_4 d_1 + d_2 + d_4$	$\delta_5 d_1 + d_3$		

To make this compatible we conclude that

$$\sigma_{b_1+b_2} = d_2 + d_3 + d_4,\ \sigma_{b_1+b_3} = d_3 + d_4,\ \sigma_{b_1+b_4} = d_4, \sigma_{b_2+b_3} = d_1 + d_3 + d_4$$
$$\sigma_{b_2+b_4} = d_1 + d_4,\ \sigma_{b_3+b_4} = d_1 + d_2 + d_4, \sigma_{b_4} = d_1 + d_2 + d_3 + d_4$$

which leaves

$b_1 + b_2 + b_3$	$b_1 + b_2 + b_4$	$b_1 + b_3 + b_4$	$b_2 + b_3 + b_4$	$b_1 + b_2 + b_3 + b_4$
$d_2 + \alpha_4 d_4$	$d_2 + \beta_5 d_3$	$\gamma_5 d_2 + d_3$	$\delta_5 d_1 + d_3$	?

and $d_2, d_3, d_1 + d_3, d_2 + d_3, d_2 + d_4$ as linear forms. (The question mark in the last table indicates that none of the projections gives any information about the value of this form.) By irreflexivity, we must have $\sigma_{b_1+b_2+b_3+b_4} \in \{d_2, d_3\}$. If $\sigma_{b_1+b_2+b_3+b_4} = d_2$, then

$$\sigma_{b_1+b_2}(b_1 + b_2 + b_3 + b_4) = 1 = \sigma_{b_1+b_2+b_3+b_4}(b_1 + b_2),$$

contradicting antisymmetry. Hence, we must have $\sigma_{b_1+b_2+b_3+b_4} = d_3$ which yields the final contradiction

$$\sigma_{b_3}(b_1 + b_2 + b_3 + b_4) = 1 = \sigma_{b_1+b_2+b_3+b_4}(b_3).$$

Hence, we have proven

Proposition 7. *The lattice of subspaces of $GF(2)^5$ does not admit an interval decomposition.*

We summarize the results of this subsection as

Theorem 3. *The lattice of subspaces of $GF(2)^n$ admits an interval decomposition if and only if $2 \leq n \leq 4$.*

4.2 GF(3)

In this subsection we will show that the situation is much richer for larger fields. In particular, we will present a structured interval decomposition of the lattice of subspaces of $GF(3)^5$. Considering only structured forms allows us to continue omitting the subscript β for the σ_p.

There is only one structured set of linear forms for $GF(3)^2$. If H_0 is a hyperplane of $GF(3)^3$, and (b_1, b_2) is an ordered basis of H_0 with (d_0, d_1, d_2) a corresponding dual basis, any such set of linear forms that is in canonical form with respect to (b_1, b_2) must satisfy $\sigma_{b_1} = d_1$. For σ_{b_2} we have three choices $d_2, d_1 + d_2$ and $2d_1 + d_2$. In turns out that we can complete all these choices to structured, irreflexive and antisymmetric sets S_1, S_2, S_3 of linear forms.

$p \in H_0$	$\sigma_p \in S_1$	$\sigma_p \in S_2$	$\sigma_p \in S_3$
b_1	d_1	d_1	d_1
b_2	d_2	$d_1 + d_2$	$d_1 + 2d_2$
$b_1 + b_2$	$d_1 + d_2$	d_2	$d_1 + d_2$
$b_1 + 2b_2$	$d_1 + 2d_2$	$d_1 + 2d_2$	d_2

We implemented the algorithm described in the last section and found 26 structured interval decompositions for the lattice of subspaces of $GF(3)^4$ and 52 for $GF(3)^5$. We list three of the former in Table 1, which are used to compute one of the latter. The full lists can be found in the Appendix of [3].

Using S_1 and S_6 once and S_3 two times as projections, we discovered the set of linear forms in Table 2.

It is possible to check by hand that these indeed are irreflexive and antisymmetric.

$p \in H_0$	$\sigma_p \in S_1$	$\sigma_p \in S_3$	$\sigma_p \in S_6$
b_1	d_1	d_1	d_1
b_2	d_2	d_2	d_2
b_3	d_3	d_3	d_3
$b_1 + b_2$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + d_3$	$d_1 + d_2$
$b_1 + 2b_2$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2 + d_3$	$d_1 + 2d_2$
$b_1 + b_3$	$d_1 + d_2 + d_3$	$d_1 + d_3$	$d_1 + 2d_2 + d_3$
$b_1 + 2b_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + 2d_3$	$d_1 + 2d_2 + 2d_3$
$b_2 + b_3$	$d_2 + d_3$	$d_1 + 2d_2 + 2d_3$	$d_1 + d_2 + d_3$
$b_2 + 2b_3$	$d_2 + 2d_3$	$d_1 + d_2 + 2d_3$	$d_1 + d_2 + 2d_3$
$b_1 + b_2 + b_3$	$d_1 + d_2$	$d_2 + d_3$	$d_1 + d_3$
$b_1 + b_2 + 2b_3$	$d_1 + 2d_3$	$d_1 + d_2$	$d_1 + 2d_3$
$b_1 + 2b_2 + b_3$	$d_1 + d_3$	$d_2 + 2d_3$	$d_2 + 2d_3$
$b_1 + 2b_2 + 2b_3$	$d_1 + 2d_2$	$d_1 + 2d_2$	$d_2 + d_3$

Table 1: Three structured interval decompositions for $GF(3)^4$

Theorem 4. *There exists an interval decomposition of the lattice of subspaces of* $GF(3)^5$*.*

5 Conclusion and Open Problems

While we could completely settle the problem of existence of interval decompositions for vector spaces of finite dimension over $GF(2)$ and over the reals, the situation seems to become more difficult for other finite fields. On the one hand the additional choices for linear forms provide a lot more flexibility and enable us to construct several interval decompositions for $GF(3)^5$, while an interval decomposition is impossible for $GF(2)^5$. On the other hand, our argument used for real vector spaces applies the Cauchy-Schwarz Inequality, which is not applicable for finite fields.

Using matching theory (see e.g. [5] Corollary 16.2b), it is immediate that there is an interval decomposition of $GF(q)^3$ for all prime powers q. Thus, finally we have the following table on the existence of interval decompositions.

Dimension	$GF(2)$	$GF(3)$	$GF(4)$	$GF(q)$, $q \geq 5$	$\mathbb{R}$
2,3	yes	yes	yes	yes	yes
4	yes	yes	yes	?	yes
5	no	yes	?	?	yes
≥ 6	no	?	?	?	yes

b_1	b_2	b_3	b_4
d_1	d_2	d_3	d_4
$b_1 + b_2$	$b_1 + 2b_2$	$b_1 + b_3$	$b_1 + 2b_3$
$d_1 + d_2 + 2d_3 + d_4$	$d_1 + 2d_2 + d_3 + d_4$	$d_1 + d_2 + d_3 + d_4$	$d_1 + 2d_2 + 2d_3 + d_4$
$b_1 + b_4$	$b_1 + 2b_4$	$b_2 + b_3$	$b_2 + 2b_3$
$d_1 + d_4$	$d_1 + 2d_4$	$d_2 + d_3$	$d_2 + 2d_3$
$b_2 + b_4$	$b_1 + 2b_4$	$b_3 + b_4$	$b_3 + 2b_4$
$d_1 + 2d_2 + d_3 + 2d_4$	$d_1 + d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3 + 2d_4$	$d_1 + d_2 + d_3 + 2d_4$
$b_1 + b_2 + b_3$	$b_1 + b_2 + 2b_3$	$b_1 + 2b_2 + b_3$	$b_1 + 2b_2 + 2b_3$
$d_1 + d_2 + 2d_4$	$d_1 + 2d_3 + 2d_4$	$d_1 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_4$
$b_1 + b_2 + b_4$	$b_1 + b_2 + 2b_4$	$b_1 + 2b_2 + b_4$	$b_1 + 2b_2 + 2b_4$
$d_2 + d_3 + d_4$	$d_1 + d_2 + d_3$	$d_2 + d_3 + 2d_4$	$d_1 + 2d_2 + 2d_3$
$b_1 + b_3 + b_4$	$b_1 + b_3 + 2b_4$	$b_1 + 2b_3 + b_4$	$b_1 + 2b_3 + 2b_4$
$d_2 + 2d_3 + 2d_4$	$d_1 + 2d_2 + d_3$	$d_2 + 2d_3 + d_4$	$d_1 + d_2 + 2d_3$
$b_2 + b_3 + b_4$	$b_2 + b_3 + 2b_4$	$b_2 + 2b_3 + b_4$	$b_2 + 2b_3 + 2b_4$
$d_1 + d_2 + d_4$	$d_1 + 2d_2 + d_4$	$d_1 + 2d_3 + d_4$	$d_1 + d_3 + d_4$
$b_1 + b_2 + b_3 + b_4$	$b_1 + b_2 + b_3 + 2b_4$	$b_1 + b_2 + 2b_3 + b_4$	$b_1 + b_2 + 2b_3 + 2b_4$
$d_1 + d_3$	$d_3 + 2d_4$	$d_1 + d_2$	$d_2 + 2d_4$
$b_1 + 2b_2 + b_3 + b_4$	$b_1 + 2b_2 + b_3 + 2b_4$	$b_1 + 2b_2 + 2b_3 + b_4$	$b_1 + 2b_2 + 2b_3 + 2b_4$
$d_1 + 2d_2$	$d_2 + d_4$	$d_1 + 2d_3$	$d_3 + d_4$

Table 2: An interval decomposition of $GF(3)^5$

We tried to fill some of the question marks by doing more extensive computations using our algorithm. We found 11 structured decompositions of $GF(4)^3$ and 53 for $GF(5)^3$. Alas, already the search for structured decompositions of $GF(4)^4$ turned out to be too costly. Imposing even more structure we managed to find six decompositions of $GF(4)^4$ with “simpler” structure, indicated by a “yes” in the table. It is impossible, though, to combine these into a decomposition of $GF(4)^5$ with that “simpler” structure.

The structured decompositions we found for $GF(3)^5$ do not seem to indicate a way to construct interval decompositions in the general case. Moreover, to our surprise, they cannot be combined into a structured decomposition of $GF(3)^6$.

Acknowledgement: The authors are grateful to an anonymous referee who pointed out a gap in an earlier version of the proof of Theorem 1.

References

[1] Ulrich Faigle, personal communication, 2004.

[2] Jay Goldman and Gian-Carlo Rota, *The number of subspaces of a vector space*, Recent Progress in Combinatorics (Proc. Third Waterloo Conf. on Combinatorics, 1968), Academic Press, New York, 1969, pp. 75–83.

[3] Steffen Hitzemann, *Über die Kombinatorik der Galoiszahlen*, Master's thesis, FernUniversität in Hagen, October 2008, p. 109.

[4] Eva Kruse, *Symmetrische Kettenzerlegungen von Verbänden und Intervallzerlegung des linearen Verbandes*, Master's thesis, Universität zu Köln, August 2004, p. 107.

[5] Alexander Schrijver, *Combinatorial optimization: Polyhedra and efficiency*, 1 ed., Springer, July 2004.