Wei-type duality theorems for matroids

Thomas Britz · Trygve Johnsen · Dillon Mayhew · Keisuke Shiromoto

Abstract We present several fundamental duality theorems for matroids and more general combinatorial structures. As a special case, these results show that the maximal cardinalities of fixed-ranked sets of a matroid determine the corresponding maximal cardinalities of the dual matroid. Our main results are applied to perfect matroid designs, graphs, transversals, and linear codes over division rings, in each case yielding a duality theorem for the respective class of objects.

Keywords Matroid duality theorems · demi-matroid · poset code · Wei's Duality Theorem · matroid design

Mathematics Subject Classification (2000) 05B35 · 06A07 · 94B05

---

Thomas Britz was supported by an ARC Discovery Grant.

T. Britz
School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail: britz@unsw.edu.au

T. Johnsen
Department of Mathematics and Statistics, University of Tromsø, N-9037 Tromsø, Norway
E-mail: trygve.johnsen@uit.no

D. Mayhew
School of Mathematics, Statistics and Operations Research, Victoria University, PO Box 600, Wellington 6140, New Zealand
E-mail: dillon.mayhew@msor.vuw.ac.nz

K. Shiromoto
Department of Mathematics and Engineering, Kumamoto University, 2-39-1, Kurokami, Kumamoto 860-8555, Japan
E-mail: keisuke@kumamoto-u.ac.jp
1 Introduction and main results

The main purpose of this paper is to present new duality theorems for matroids; see Theorems 1-3 below in this section. We also present duality theorems for more general combinatorial structures that we call demi-matroids; see Theorems 5 and 6 in Section 2. These new combinatorial structures provide the natural and exact framework for duality results such as Wei's celebrated Duality Theorem [14]. The main theorems are applied in Section 3 to the classes of perfect matroid designs, graphs, transversals, and linear codes over division rings, in each case yielding a duality theorem for the particular class of objects in question. One of these duality theorems is a strong poset-code generalization of Wei's celebrated Duality Theorem [14] as well as of previous generalizations thereof; see Theorem 11. Our derivation of these coding-theoretical results shows that they are essentially combinatorial in nature. Our results also shed new light on perfect matroid designs. In particular, we show that the closed-set cardinalities of a perfect matroid design are uniquely determined by corresponding cardinalities of the matroid dual; see Theorem 7.

Let $M = (E, \rho)$ be a matroid with rank $k := \rho(M)$ on a finite set $E$ of $n$ elements. For each $i = 0, \ldots, k$ and $j = 0, \ldots, n - k$, define

$$f_i := \max\{|F| : F \subseteq E, \rho(F) = i\};$$

$$f_j^* := \max\{|F| : F \subseteq E, \rho^*(F) = j\},$$

and set

$$S_M := \{n - f_{k-1}, \ldots, n - f_0\};$$

$$T_M := \{f_0^*, \ldots, f_{n-k-1}^* + 1\}.$$

The first and simplest of our duality theorems is Theorem 1 below. It states that the sets $S_M$ and $T_M$ partition the set $\{1, \ldots, n\}$ and thereby determine each other.

**Theorem 1** $S_M \cup T_M = \{1, \ldots, n\}$ and $S_M \cap T_M = \emptyset$.

**Example 1** The Vamos matroid $M := V_5$ on $E := \{1, \ldots, 8\}$ is simple, self-dual, non-uniform, and paving, so $(f_0, f_1, f_2, f_3) = (f_0^*, f_1^*, f_2^*, f_3^*) = (0, 1, 2, 4)$. It follows that $S_M = \{4, 6, 7, 8\}$ and $T_M = \{1, 2, 3, 5\}$. Thus, $S_M \cup T_M = \{1, \ldots, 8\}$ and $S_M \cap T_M = \emptyset$, as asserted by Theorem 1.

Theorem 1 is a special case of Theorem 2 below. In order to express the latter theorem and its companion, Theorem 3, we must introduce some further notation.

Let $P$ be a partially ordered set (poset) with elements $E$ and order relation $\leq_P$. The dual of $P$ is the poset $\overline{P}$ on $E$ with order relation $\leq_{\overline{P}}$ defined for all $x, y \in E$ by $x \leq_{\overline{P}} y$ if and only if $y \leq_P x$. For each subset $A \subseteq E$, let $(A)_P$ denote the order ideal $\{x \in E : x \leq_P y \text{ for some } y \in A\}$. Note that if $P$ is an antichain (i.e., when $P = \overline{P}$), then $(A)_P = A$. 
For all $i = 0, \ldots, k$ and $j = 0, \ldots, n - k$, define

\[ \phi_i^P := \min\{ |\{F\}_P| : F \subseteq E, \rho(F) = i \}; \]
\[ \phi_j^{P,*} := \min\{ |\{F\}_P| : F \subseteq E, \rho^*(F) = j \}; \]
\[ f_i^P := \max\{ |E - \{E - F\}_P| : F \subseteq E, \rho(F) = i \}; \]
\[ f_j^{P,*} := \max\{ |E - \{E - F\}_P| : F \subseteq E, \rho^*(F) = j \}. \]

Set

\[ S_M^P := \{n - f_{k-1}^P, \ldots, n - f_0^P\}; \]
\[ T_M^P := \{f_0^{P,*} + 1, \ldots, f_{n-k-1}^{P,*} + 1\}; \]
\[ U_M^P := \{\phi_1^P, \ldots, \phi_k^P\}; \]
\[ V_M^P := \{n + 1 - \phi_{n-k}^{P,*}, \ldots, n + 1 - \phi_1^{P,*}\}. \]

The main results of this paper are presented in Theorems 2 and 3 below.

**Theorem 2** $S_M^P \cup T_M^P = \{1, \ldots, n\}$ and $S_M^P \cap T_M^P = \emptyset$.

**Theorem 3** $U_M^P \cup V_M^P = \{1, \ldots, n\}$ and $U_M^P \cap V_M^P = \emptyset$.

Note that $S_M = S_M^P$ and $T_M = T_M^P$ whenever $P$ is an antichain. Thus, Theorem 1 follows immediately from Theorem 2; an independent proof of Theorem 1 is also to be found in [8]. Theorems 2 and 3 in turn follow from more general duality theorems for demi-matroids, namely Theorems 5 and 6 in Section 2.

**Remark 1** If $P$ is an antichain, then $\phi_i^P = i$ and $\phi_j^{P,*} = j$ for all integers $i = 0, \ldots, k$ and $j = 0, \ldots, n - k$, so $U_M^P = \{1, \ldots, k\}$ and $V_M^P = \{k + 1, \ldots, n\}$. Thus, whereas Theorem 2 implies Theorem 1, Theorem 3 does not imply any similarly interesting result for matroids. The next section, however, will introduce more general objects ("demi-matroids") for which the associated generalization of Theorem 3 (Theorem 6) will be shown to be just as interesting as the associated generalization of Theorem 2 (Theorem 5); see Lemma 4.

## 2 Wei-type duality theorems for demi-matroids

The duality theorems expressed in Theorems 1-3 are not unique to matroids but are more generally, and more naturally, satisfied by new combinatorial objects that we introduce in this section. In particular, a demi-matroid is a triple $(E, s, t)$ consisting of a finite set $E$ and two functions $s, t : 2^E \to \mathbb{N}_0$ satisfying the following two conditions for all subsets $X \subseteq Y \subseteq E$:

(R) $0 \leq s(X) \leq s(Y) \leq |Y|$ and $0 \leq t(X) \leq t(Y) \leq |Y|$;
(D) $|E - X| - s(E - X) = t(E) - t(X)$.
Note that \( s(\emptyset) = t(\emptyset) = 0 \) by (R). Thus, (D) is equivalent to the following condition:

\[(D') \quad |E - X| - t(E - X) = s(E) - s(X).\]

Note that for any matroid \( M = (E, \rho) \) on \( E \), the triple \( (E, \rho, \rho^*) \) is a demi-matroid. Conversely, if \( (E, s, t) \) is a demi-matroid, then \( s \) is the rank function of a matroid \( M \) on \( E \) if and only if \( t \) is the rank function of \( M^* \). The following example shows that demi-matroids properly generalize matroids.

**Example 2** Suppose that \( E = \{a, b\} \), and define and \( s(E) := 1 \) and \( s(X) := 0 \) for each subset \( X = \emptyset, \{a\}, \{b\} \). The triple \( (E, s, t) \) is a demi-matroid but \( s \) is not the rank function of any (poly)matroid on \( E \).

Let \( D = (E, s, t) \) be a demi-matroid on \( E \). By (D), \( s(E) + t(E) = n \). Set \( k := s(E) \).

**Lemma 1** \( s(X - x) \geq s(X) - 1 \) and \( t(X - x) \geq t(X) - 1 \) for all \( X \subseteq E \) and \( x \in E \).

**Proof.** By (R) and (D),

\[
t(X - x) = t(E) - |E - (X - x)| + s(E - (X - x)) \\
\geq t(E) - |E - X| - 1 + s(E - X) \\
= t(X) - 1.
\]

Similarly, \( s(X - x) \geq s(X) - 1 \).

Let \( P \) be a poset as described in the Introduction, and define for each \( i = 0, \ldots, k \) and \( j = 0, \ldots, n - k \),

\[
\sigma_i^P := \min\{|(X)_p| : X \subseteq E, s(X) \geq i\}; \\
\tau_j^P := \min\{|(X)_p| : X \subseteq E, t(X) \geq j\}; \\
s_i^P := \max\{|E - (E - X)_p| : X \subseteq E, s(X) \leq i\}; \\
t_j^P := \max\{|E - (E - X)_p| : X \subseteq E, t(X) \leq j\}.
\]

By (R) and Lemma 1, all of the numbers \( \sigma_i^P, \tau_j^P, s_i^P, \) and \( t_j^P \) are well-defined and may be given the following equivalent characterizations.

**Lemma 2** For all \( i = 0, \ldots, k \) and \( j = 0, \ldots, n - k \),

\[
\sigma_i^P = \min\{|(X)_p| : X \subseteq E, s(X) = i\}; \\
\tau_j^P = \min\{|(X)_p| : X \subseteq E, t(X) = j\}; \\
s_i^P = \max\{|E - (E - X)_p| : X \subseteq E, s(X) = i\}; \\
t_j^P = \max\{|E - (E - X)_p| : X \subseteq E, t(X) = j\}.
\]
Remark 2 If $P$ is an antichain, then
\[ s_i^P = \max\{ |X| : X \subseteq E, s(X) = i \} \quad \text{and} \quad t_j^P = \max\{ |X| : X \subseteq E, t(X) = j \}. \]

If, in addition, $M = (E, \rho)$ is a matroid on $E$, then the coefficients $\sigma_i^P, \tau_j^P$ for the demi-matroid $D := (E, \rho, \rho^*)$ are trivial: $\sigma_i^P = i$ and $\tau_j^P = j$ for all relevant $i, j$.

Lemma 3 The following inequalities hold:
\begin{align*}
0 &= \sigma_0^P < \sigma_1^P < \sigma_2^P < \cdots < \sigma_k^P \leq n; \\
0 &= \tau_0^P < \tau_1^P < \tau_2^P < \cdots < \tau_{n-k}^P \leq n; \\
0 &\leq s_0^P < s_1^P < s_2^P < \cdots < s_k^P = n; \\
0 &\leq t_0^P < t_1^P < t_2^P < \cdots < t_{n-k}^P = n.
\end{align*}

Proof. For any $i = 1, \ldots, k$, let $X \subseteq E$ be a subset such that $|(X)_{\rho}| = \sigma_i^P$ and $s(X) \geq i$. Then $X \neq \emptyset$ since $s(X) \geq 1$. Choose an element $x \in X$ that is maximal in $P$. Then $(X - x)_{\rho} \subseteq (X)_{\rho}$. By Lemma 1, $s(X - x) \geq i - 1$, so $\sigma_{i-1}^P \leq |(X - x)_{\rho}| < |(X)_{\rho}| = \sigma_i^P$.

The remaining inequalities follow similarly. \qed

Lemma 3 induces the following Singleton-type bounds.

Corollary 1 For all $i = 0, \ldots, k$ and $j = 0, \ldots, n - k$,
\begin{align*}
\sigma_i^P &\leq n - k + i, & \tau_j^P &\leq k + j, & \sigma_j^P &\leq n - k + i, & t_j^P &\leq k + j.
\end{align*}

The dual demi-matroid of a demi-matroid $D := (E, s, t)$ is the triple $D^* := (E, t, s)$. The operation $D \to D^*$ is clearly an involution, i.e., $D = (D^*)^*.$

A second fundamental involution on demi-matroids is now presented. For any real function $f : 2^E \to \mathbb{R}$, let $\overline{f}$ denote the function given by
\[ \overline{f}(X) := f(E) - f(E - X). \]
Since $\overline{f}(X) = \overline{f}(E) - \overline{f}(E - X) = f(X) - f(\emptyset)$, it follows that if $f(\emptyset) = 0$, then the operation $f \to \overline{f}$ is an involution, i.e., $f = \overline{f}$.

Theorem 4 The triple $D := (E, \emptyset, t)$ is a demi-matroid; also, $D = \overline{D}$ and $D^* = \overline{D}^*.$

Proof. Routine verification shows that $\overline{D}$ is a demi-matroid. To conclude, note that $D = (E, s, t) = (E, \emptyset, \overline{t}) = \overline{D}$ and $D^* = (E, t, s) = (E, \emptyset, \overline{s}) = (E, \emptyset, \overline{t})^* = \overline{D}^*.$ \qed

The demi-matroid $\overline{D}$ is called the supplement of $D$. 

Example 3 The supplement of a matroid is not necessarily a matroid. For instance, consider the matroid \( M := (E, \rho) \) consisting of a loop and two parallel elements. Then \( D := (E, \rho, \rho^*) \) is a demi-matroid, so \( \bar{D} = (E, \bar{\rho}, \bar{\rho}^*) \) is also a demi-matroid. However, \( (E, \bar{\rho}) \) is not a matroid, since it would have rank 1 but only contain loops.

Define for all \( i = 0, \ldots, k \) and \( j = 0, \ldots, n - k \),
\[
\sigma_i^P := \min\{ |(X) p| : X \subseteq E, \bar{s}(X) \geq i \}; \\
\tau_j^P := \min\{ |(X) p| : X \subseteq E, \bar{t}(X) \geq j \}; \\
\bar{s}_i^P := \max\{ |E - (E - X) p| : X \subseteq E, \bar{s}(X) \leq i \}; \\
\bar{t}_j^P := \max\{ |E - (E - X) p| : X \subseteq E, \bar{t}(X) \leq j \}.
\]

Lemma 4 For all \( i = 0, \ldots, k \) and \( j = 0, \ldots, n - k \),
\[
s_i^P = n - \sigma_{i-k}^P; \quad t_j^P = n - \tau_{n-k-j}^P; \quad \sigma_i^P = n - \bar{s}_{i-k}^P; \quad \tau_j^P = n - \bar{t}_{n-k-j}^P.
\]

Proof. It is easy to show that, for each \( i = 0, \ldots, k \),
\[
s_i^P = \max\{ |E - (E - X) p| : X \subseteq E, s(X) = i \}; \\
\bar{s}_i^P = \max\{ |(X) p| : X \subseteq E, \bar{s}(X) = i \}.
\]
Then
\[
s_i^P = \max\{ |E - (E - X) p| : X \subseteq E, s(E - X) = i \} \\
= n - \min\{ |(X) p| : X \subseteq E, \bar{s}(X) = k - i \} \\
= n - \sigma_{k-i}^P.
\]
The remaining identities are proved similarly. \( \square \)

Set
\[
S_D^P := \{n - s_{k-1}^P, \ldots, n - s_k^P\}; \\
T_D^P := \{t_0^P + 1, \ldots, t_{n-k-1}^P + 1\}; \\
U_D^P := \{\sigma_1^P, \ldots, \sigma_k^P\}; \\
V_D^P := \{n + 1 - \tau_{n-k}^P, \ldots, n + 1 - \tau_1^P\}.
\]

Lemma 4 implies the following identities.

Lemma 5 \( S_D^P = U_D^P \) and \( T_D^P = V_D^P \).

The strongest results of this paper are Theorems 5 and 6 below. Note that these results immediately imply Theorems 2 and 3.

Theorem 5 \( S_D^P \cup T_D^P = \{1, \ldots, n\} \) and \( S_D^P \cap T_D^P = \emptyset \).
Theorem 6 \( U_D^P \cup V_D^P = \{1, \ldots, n\} \) and \( U_D^P \cap V_D^P = \emptyset \).

Proof of Theorems 5 and 6. Assume that \( \sigma_i^P = n + 1 - \tau_j^P \), and let \( X \subseteq E \) be a subset satisfying \(|(X)_p| = \sigma_i^P \) and \( s(X) \geq i \). Now, set \( Y := E - (X)_p \) and note that \( Y \) is an ideal in \( P \). Then \(|(Y)_p| = |Y| = n - \sigma_i^P = \tau_j^P - 1 \), so \( t(Y) \leq j - 1 \). By (R) and (D),
\[
\begin{align*}
n - k - \sigma_i^P + i & \leq t(E) - |(X)_p| + s(X) \\
& \leq t(E) - |(X)_p| + s((X)_p) \\
& = t(E) - |E - Y| + s(E - Y) \\
& = t(Y) \\
& \leq j - 1.
\end{align*}
\]
Similarly, \( n - (n - k) - \tau_j^P + j \leq i - 1 \). Hence, \( -1 = n - \sigma_i^P - \tau_j^P \leq -2 \), which is a contradiction. It follows that \( \sigma_i^P \neq n + 1 - \tau_j^P \) for all \( i, j \). This proves Theorem 6.

To prove Theorem 5, apply Theorem 6 to \( \overline{D} \), and use Lemma 5. \( \square \)

Example 4 For the demi-matroid \( D := (E, s, t) \) with \( E = \{a, b, c\} \), \( s(E) = 1 \), and \( s(X) = 0 \) for \( X \subseteq E \), and an antichain \( P \) on \( E \),
\[
S_D^P = \{1\}, \quad T_D^P = \{2, 3\}, \quad U_D^P = \{3\}, \quad \text{and} \quad V_D^P = \{1, 2\}.
\]
Thus, \( S_D^P \cup T_D^P = \{1, 2, 3\} \) and \( S_D^P \cap T_D^P = \emptyset \), as asserted by Theorem 5. Likewise, \( U_D^P \cup V_D^P = \{1, 2, 3\} \) and \( U_D^P \cap V_D^P = \emptyset \), as asserted by Theorem 6. Here we see that Theorems 5 and 6 give results that cannot be obtained directly from Theorems 2 and 3, since \((E, s)\) and \((E, t)\) are not matroids.

3 Duality theorems for particular classes of objects

The duality theorems (Theorems 1, 2, 3, 5, and 6) presented in the previous sections may each be applied to numerous classes of objects that induce matroids and demi-matroids, thus yielding duality theorems for each of these classes. In this section, we apply these matroid and demi-matroid theorems to the classes of perfect matroid designs, graphs, transversals, and linear codes.

In the following, let \( P \) be a partial order on the set \( E \). It is not difficult to show that if \( M \) is a matroid on \( E \) with rank \( k \) and coefficients \( f_i^P \) and \( f_j^{P,*} \), then
\[
\begin{align*}
n - f_{k-i}^P &= \min\{|(X)_p| : X \subseteq E \text{ is a union of } i \text{ cocircuits of } M, \quad (F) \}
\quad \text{\( \text{none contained in the union of the others}\)}; \\
n - f_{n-k-j}^{P,*} &= \min\{|(X)_p| : X \subseteq E \text{ is a union of } j \text{ circuits of } M, \quad (F') \}
\quad \text{\( \text{none contained in the union of the others}\)}.
\end{align*}
\]
3.1 Perfect matroid designs

A perfect matroid design is a matroid \( M \) in which the cardinality of each closed set is determined uniquely by its rank (see [15, Chapter 12] and [5]). If the rank of a closed set \( F \) of \( M \) is \( i \), then \( |F| = f_i \). Theorem 1 immediately implies the following result.

**Theorem 7** The cardinalities of the closed sets of a perfect design matroid \( M \) are uniquely determined by the maximal cardinalities, for all \( j \), of the \( j \)-ranked closed sets of \( M^* \).

3.2 Graphs

Let \( G \) be a (multi)graph on \( n \) edges \( E \) whose spanning forests each contains \( k \) edges, and let \( P \) be a poset on \( E \). Recall that a bond of \( G \) is a minimal cut-set of edges of \( G \). For each \( i = 1, \ldots, k \) and \( j = 1, \ldots, n - k \), define

\[
\begin{align*}
b_i^P := & \min\{|(X)_P| : X \subseteq E \text{ is a union of } i \text{ bonds of } G, \\
& \text{none of which are contained in the union of the others}\}; \\
c_j^P := & \min\{|(X)_P| : X \subseteq E \text{ is a union of } j \text{ cycles of } G, \\
& \text{none of which are contained in the union of the others}\}.
\end{align*}
\]

Consider the cycle matroid \( M := M(G) \) and its coefficients \( f_i^P \) and \( f_j^{P,*} \). Equations (F) and (F') immediately imply the following result.

**Proposition 1** \( b_i^P = n - f_{k-i}^P \) and \( c_j^P = n - f_{n-k-j}^{P,*} \).

Set

\[
\begin{align*}
S^P_G := & \{b_1^P, \ldots, b_k^P\}; \\
T^P_G := & \{n + 1 - c_{n-k}^P, \ldots, n + 1 - c_1^P\}.
\end{align*}
\]

The next result generalizes [3, Theorem 13] and follows immediately from Theorem 1 and Proposition 1.

**Theorem 8** \( S^P_G \cup T^P_G = \{1, \ldots, n\} \) and \( S^P_G \cap T^P_G = \emptyset \).

**Example 5** The graph \( G \) below has \( n = 5 \) edges \( E = \{1, 2, 3, 4, 5\} \), and each of its spanning forests has \( k = 3 \) edges:
Let $P$ be the antichain on $E$. Then $(b_1^P, b_2^P, b_3^P) = (2, 4, 5)$ and $(c_1^P, c_2^P) = (3, 5)$. Set

\[
S_G^P := \{b_1^P, b_2^P, b_3^P\} = \{2, 4, 5\};
\]

\[
T_G^P := \{n + 1 - c_2^P, n + 1 - c_1^P\} = \{1, 3\}.
\]

Then $S_G^P \cup V_G^P = \{1, 2, 3, 4, 5\}$ and $T_G^P \cap V_G^P = \emptyset$, as asserted by Theorem 8.

3.3 Transversals

Let $A := \{A_1, \ldots, A_m\}$ be a multiset of subsets $A_j \subseteq E$. A transversal, or matching, of $A$ is a set $T \subseteq E$ of size $|T| = |A|$ for which the elements of $T$ may be labeled $e_1, \ldots, e_m$ so that $e_j \in A_j$ for each $j = 1, \ldots, m$. A partial transversal of $A$ is a transversal of a sub-multiset of $A$. The partial transversals of $A$ form the independent sets of the transversal matroid of $A$, denoted by $M[A]$ (cf. [15, Section 1.6]). A set $X \subseteq E$ is a plug for $A$ if $X - e$ is a partial transversal of $A$ for each $e \in X$ but $X$ itself is not. Let $k$ denote the maximal size of a partial transversal of $A$, that is, the rank of $M[A]$. For each $i = 0, \ldots, k - 1$ and $j = 1, \ldots, n - k$, define

\[
p_i^P := \min\{|(X)_j| : X \subseteq E \text{ is a union of } i \text{ plugs for } A,
\text{ none contained in the union of the others.}\}.
\]

\[
m_j^P := \max\{|(X)_j| : X \subseteq E \text{ contains a partial transversal of } A \text{ of size } j
\text{ but none of size } j + 1\}.
\]

Set

\[
S_A^P := \{p_1^P, \ldots, p_{n-k}^P\} ;
\]

\[
T_A^P := \{m_0^P + 1, \ldots, m_{k-1}^P + 1\}.
\]

Theorem 9 $S_A^P \cup T_A^P = \{1, \ldots, n\}$ and $S_A^P \cap T_A^P = \emptyset$.

Proof. For $M := (M[A])^*$ with rank $n - k$, $p_i^P = n - f_{n-k-i}$ and $m_i^P = f_{k-i}$, by (F'). Use Theorem 2. $\square$

Example 6 Let $E := \{a, b, c, d, e\}$ and $A := \{\{a, b\}, \{a, c\}, \{d\}, \{d\}\}$. Then for the antichain $P$ on $E$, $S_A^P = \{1, 3\}$ and $T_A^P = \{2, 4, 5\}$. Therefore, $S_A^P \cup T_A^P = \{1, 2, 3, 4, 5\}$ and $S_A^P \cap T_A^P = \emptyset$, as claimed by Theorem 9.

3.4 Codes over division rings

Let $R$ denote a division ring (possibly a field). The (Hamming) support of each codeword $x := (x_1, \ldots, x_n) \in R^n$ and each subset $D \subseteq R^n$ are the sets

\[\text{supp}(x) := \{i \in E : x_i \neq 0\} \quad \text{and} \quad \text{Supp}(D) := \bigcup_{x \in D} \text{supp}(x).\]
Let $P$ be a poset on $E$. The $P$-weight of each subset $D \subseteq R^n$ is defined as follows:

$$\text{wt}_P(D) := |\langle \text{Supp}(D) \rangle_P|.$$

Let $C$ be a right linear $[n,k]$ code over $R$ with coordinates $E$. The dual code $C^\perp$ is given as follows:

$$C^\perp := \{ y \in R^n : x \cdot y = 0 \text{ for all } x \in C \}.$$

For each integer $i = 1, \ldots, k$ ($j = 1, \ldots, n-k$), define the $i$th ($j$th) generalized $P$-weight of $C$ ($C^\perp$) as follows:

$$d_i^P := \min \{ \text{wt}_P(D) : D \subseteq C, \dim D = i \} ;$$

$$d_j^{P,\perp} := \min \{ \text{wt}_{P^\perp}(D) : D \subseteq C^\perp, \dim D = j \} .$$

For any subset $X \subseteq E$, the punctured code $C \setminus X$ is the right linear code obtained by deleting the coordinates $X$ from each codeword of $C$. Also, $C(X)$ is the right linear subcode of $C$ consisting of all codewords $x \in C$ for which $\text{supp}(x) \subseteq X$. Note that $k = \dim C = \dim C \setminus X + \dim C(X)$.

Define the function $\rho_C : 2^E \rightarrow N_0$ by

$$\rho_C(X) := \dim C \setminus (E \setminus X) .$$

This is the rank function of the vector matroid $M_C = (E, \rho_C)$. Define $\rho_{C^\perp}$ similarly for $C^\perp$ and note that $\rho_C^\perp = \rho_{C^\perp}$.

**Theorem 10** $D_C := (E, \rho_C, \rho_{C^\perp})$ is a demi-matroid.

Consider the numbers $\sigma_i^P$ and $\tau_j^{P,\perp}$ associated to $D_C$.

**Proposition 2** $d_i^P = \sigma_i^P = n - s_{k-i}$ and $d_j^{P,\perp} = \tau_j^{P,\perp} = n - t_{n-k-j}$.

**Proof.** Let $D$ be a right linear $[n,i]$ subcode of $C$ for which $\text{wt}_P(D) = d_i^P(C)$. Then for $X := \text{Supp}(D)$, $\rho_C(X) = k - \rho_C(E \setminus X) = \dim D = i$, so $d_i^P = \text{wt}_P(D) = |\langle X \rangle_P| \geq \sigma_i^P$.

Conversely, let $X \subseteq E$ be a subset with $\rho_C(X) = i$ and $|\langle X \rangle_P| = \sigma_i^P$. Now, $C(X)$ is a right linear subcode of $C$ with $\dim C(X) = k - \rho_C(E \setminus X) = \rho_C(X) = i$. Hence, $d_i^P \leq \text{wt}_P(C(X)) \leq |\langle X \rangle_P| = \sigma_i^P$.

It follows that $d_i^P = \sigma_i^P$. Similarly, $d_j^{P,\perp} = \tau_j^{P,\perp}$, and Lemma 4 concludes the proof.

Set

$$S_C^P := \{ d_1^P, \ldots, d_k^P \} ;$$

$$T_C^{P,\perp} := \{ n - d_{n-k}^{P,\perp}, \ldots, n - d_1^{P,\perp} \}.$$

**Theorem 11** $S_C^P \cup T_C^{P,\perp} = \{1, \ldots, n\}$ and $S_C^P \cap T_C^{P,\perp} = \emptyset$.

**Proof.** Use Theorems 5 and 10 together with Proposition 2. □
Example 7 Consider the linear code $C$ generated by the following binary matrix:

$$
\begin{pmatrix}
1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 \\
\end{pmatrix}
$$

Here, $R = \text{GF}(2)$, $E = \{1, 2, 3, 4, 5\}$, $n = 5$, and $k = 3$. Let $P$ be the partially ordered set on $E$, with order relation $\preceq_P$ determined by the inequalities $4 \preceq_P 1, 2, 3 \preceq_P 5$. Then $(d_1^P, d_2^P, d_3^P) = (3, 4, 5)$ and $(d_1^{P,c}, d_2^{P,c}) = (4, 5)$, so $S_C^P = \{3, 4, 5\}$ and $T_C^P = \{1, 2\}$. Hence, $S_C^P \cap T_C = \emptyset$ and $S_C^P \cup T_C^P = \{1, 2, 3, 4, 5\}$, as asserted by Theorem 11.

Theorem 11 above extends slightly the recent poset-code generalization of Wei's Duality Theorem by Barg and Purkayastha [2] and Moura and Firer [9]. Their generalization is obtained from Theorem 11 by letting $R$ be a finite field. This shows that Wei's Duality Theorem and its above-mentioned generalization are essentially combinatorial in nature.

Note also that Theorem 11 does not extend the duality results by Ashikhmin [1] and Horimoto and Shiromoto [7] for linear codes over Galois- and chain rings. It remains an open problem to find poset-code generalizations for such results.

3.4.1 Ordered Hamming spaces

The ordered Hamming space, also called the Niederreiter-Rosenbloom-Tsfasman metric space, is the set of $r \times c$ matrices $R^{r \times c}$ over the division ring $R$ endowed with the metric $d_L(x, y) := \text{wt}_L(x - y)$ for all $x, y \in R^{r \times c}$, where

$$
\text{wt}_L(x) := \sum_{i=1}^{r} \max\{j \in \{1, \ldots, c\} : x_{ij} \neq 0\}.
$$

The matrices $x \in R^{r \times c}$ are often represented as concatenated vectors, or blocks, each of length $c$:

$$
x = (x_{11}, \ldots, x_{1c}; \ldots; x_{r1}, \ldots, x_{rc}).
$$

Ordered Hamming spaces were implicitly introduced in [10–12, 16]. As first noted in [4], these spaces may be viewed as poset codes with $P_o$-weight $\text{wt}_{P_o}(x) = \text{wt}_L(x)$, where $P_o$ is a poset consisting of a disjoint union of $r$ chains, each corresponding to a row (or block) of $x$; this observation indeed led to the notion of poset codes. Dualizing the poset $P_o$, one obtains a second weight function $\text{wt}_R(x) = \text{wt}_{P^c}(x)$ given explicitly as follows:

$$
\text{wt}_R(x) := \sum_{i=1}^{r} (c + 1 - \min\{j \in \{1, \ldots, c\} : x_{ij} \neq 0\})
$$

.$$
Let $C \subseteq R^{x \times c}$ be a right linear $[n, k]$-code, where $n = rc$, and let $C^\perp \subseteq R^{x \times c}$ be the dual code of $C$. For each integer $i = 1, \ldots, k$ ($j = 1, \ldots, n - k$), define the $i$th left-ordered weight of $C$ ($j$th right-ordered weight of $C^\perp$) as follows:

$$d^L_i := \min \{ \text{wt}_L(D) : D \subseteq C, \ \dim D = i \} ;$$

$$d^{R,\perp}_j := \min \{ \text{wt}_R(D) : D \subseteq C^\perp, \ \dim D = j \} .$$

Set

$$S^C_e := \{ d^L_1, \ldots, d^L_k \} ;$$

$$T^C_e := \{ n + 1 - d^{R,\perp}_{n-k}, \ldots, n + 1 - d^{R,\perp}_1 \} .$$

The following theorem expresses the ordered Hamming space generalization of Wei's Duality Theorem and follows immediately from Theorem 11 and the identities

$$S^C_e = S^R_{\overline{c}} \quad \text{and} \quad T^C_e = T^R_{\overline{c}} .$$

**Theorem 12** $S^C_e \cup T^C_e = \{ 1, \ldots, n \}$ and $S^C_e \cap T^C_e = \emptyset$.

The above theorem reduces to Wei’s Duality Theorem [14] when $c = 1$; that is, when $P$ is an antichain.

**Example 8** Consider the linear code $C$ spanned by the following two binary matrices:

$$
\begin{pmatrix}
0 & 1 \\
0 & 0
\end{pmatrix} \quad \begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}
$$

In this example, $R = GF(2)$, $n = 4$, and $k = 2$. Furthermore, $(d^L_1, d^L_2) = (d^{R,\perp}_1, d^{R,\perp}_2) = (2, 4)$. Then $L_C = \{ 2, 4 \}$ and $R_C = \{ 1, 3 \}$, so $L_C \cap R_C = \emptyset$ and $L_C \cup R_C = \{ 1, 2, 3, 4 \}$, as asserted by Theorem 12.

**Acknowledgements** We gratefully thank Allan Moura and Marcelo Firer for sending us a preprint of their article [9] and we thank Alexander Barg for drawing our attention to their result. We also thank the referees for their excellent comments and suggestions.

**References**