<table>
<thead>
<tr>
<th>Title</th>
<th>An Assmus-Mattson Theorem for Matroids (Theory and Applications of Combinatorial Designs with Related Field)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>SHIROMOTO, Keisuke</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2006), 1465: 71-76</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2006-01</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/48037">http://hdl.handle.net/2433/48037</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
An Assmus-Mattson Theorem for Matroids

Keisuke SHIROMOTO
Department of Information Systems
Aichi Prefectural University
Nagakute, Aichi 480-1198, JAPAN;
keisuke@ist.aichi-pu.ac.jp

Abstract
This note is a summary of the results in the preprints [2], [3] and [4] which are the joint works with Thomas Britz.

1 Introduction

The most celebrated result to connect coding theory and design theory is undoubtedly the Assmus-Mattson Theorem [1]. It offers a sufficient condition for the codewords of a given weight in a linear code over a finite field to form a simple \( t \)-design. Consequently, it has been used to construct \( t \)-designs from linear codes; for instance, 5-designs are in [1] obtained from the extended Golay code, the extended ternary Golay code, and other codes.

The MacWilliams identity [8] for the weight enumerator of a linear code over a finite field plays an important role in the proof of the Assmus-Mattson Theorem. Recently [2], we proved a matroid theoretical analogue of this identity. In [3], we apply this MacWilliams identity for matroids in order to establish the matroid theoretical analogue of the Assmus-Mattson theorem. We prove the Assmus-Mattson theorem for subcode supports of linear codes in [4].

Our matroid theoretic terminology essentially follows that of Whitney [13], Tutte [11], Oxley [10] and Welsh [12].

2 Notation and Terminology

We begin by introducing matroids, as in [10]. A matroid is an ordered pair \( M = (E, \mathcal{I}) \) consisting of a finite set \( E \) and a collection \( \mathcal{I} \) of subsets of \( E \) satisfying the following three conditions:

(I1) \( \emptyset \in \mathcal{I} \).

(I2) If \( I \in \mathcal{I} \) and \( I' \subseteq I \), then \( I' \in \mathcal{I} \).
(I3) If $I_1$ and $I_2$ are in $\mathcal{I}$ and $|I_1| < |I_2|$, then there is an element $e$ of $I_2 - I_1$ such that $I_1 \cup e \in \mathcal{I}$.

The members of $\mathcal{I}$ are the independent sets of $M$, and a subset of $E$ that is not in $\mathcal{I}$ is called dependent. A minimal dependent set in $M$ is called a circuit of $M$, and a maximal independent set in $M$ is called a base of $M$. For a subset $X$ of $E$, we define the rank of $X$ as follows:

$$\rho(X) := \max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\}.$$

The dual matroid $M^*$ of $M$ is defined as the matroid, the set of bases of which is

$$\{E - B : B \text{ is a base of } M\}.$$

When we denote the rank of $M^*$ by $\rho^*$, the following is well-known:

$$\rho^*(X) = |X| - \rho(M) + \rho(E - X).$$

For a matroid $M = (E, \mathcal{I})$ and a subset $T$ of $E$, it is easy to check that

$$M \backslash T = (E - T, \{I \subseteq E - T : I \in \mathcal{I}\})$$

is a matroid which is called the deletion of $T$ from $M$. The contraction of $T$ from $M$ is given by

$$M/T = (M^* \backslash T)^*.$$

For an $m \times n$ matrix $A$ over $\mathbb{F}_q$, if $E$ is the set of column labels of $A$ and $\mathcal{I}$ is the set of subsets $X$ of $E$ for which the multiset of columns labeled by $X$ is linearly independent in the vector space $\mathbb{F}_q^m$, then $M[A] := (E, \mathcal{I})$ is a matroid and is called a matroid of $A$ over $\mathbb{F}_q$.

For a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and a subset $D \subseteq \mathbb{F}_q^n$, we define the supports of $\mathbf{x}$ and $D$ respectively as follows:

$$\text{supp}(\mathbf{x}) := \{i | x_i \neq 0\},$$

$$\text{Supp}(D) := \bigcup_{\mathbf{x} \in D} \text{supp}(\mathbf{x}).$$

A $t$-$(v, k, \mu)$ design is a collection $\mathcal{B}$ of $k$-subsets (called blocks) of a set $V$ with $v$ points, such that any $t$-subset of $V$ is contained in exactly $\mu$ blocks. In [1], E. F. Assmus, Jr. and H. F. Mattson, Jr. proved the following result, which is thus widely known as the Assmus-Mattson Theorem (cf. [7]).

**Theorem 2.1** Let $C$ be a linear code on $E$ over $\mathbb{F}_q$ with minimum nonzero weight $d$, and let $d^\perp$ denote the minimum nonzero weight of $C^\perp$. Let $w = n$ when $q = 2$ and otherwise let $w$ be the largest integer satisfying

$$w - \left\lfloor \frac{w + q - 2}{q - 1} \right\rfloor < d,$$

defining $w^+$ similarly. Suppose there is an integer $t$ with $0 < t < d$ that satisfies the following condition: the number of indices $i$ $(1 \leq i \leq n - t)$ such that $A_{C^\perp}(i) \neq 0$ is at most $d - t$. Then for each $i$ with $d \leq i \leq w$, the supports of codewords in $C$ of weight $i$, provided there are any, yield a $t$-design. Similarly, for each $j$ with $d^\perp \leq j \leq \min\{w^+, n - t\}$, the supports of codewords in $C^\perp$ of weight $j$, provided there are any, form a $t$-design.
3 Main Results

For any subset $T \subseteq E$ and a matroid $M$, let $M.T$ denote the contraction $M/(E - T)$ and let $M|T$ denote the deletion $M \setminus (E - T)$. The characteristic polynomial $p(M; \lambda)$ of a matroid $M$ on the set $E$ is given by the sum

$$p(M; \lambda) = \sum_{T \subseteq E} (-1)^{|T|} \lambda^{\rho(E) - \rho(T)},$$

where $\rho$ is the rank function of $M$.

The characteristic enumerator of a matroid $M$ on a set $E$ is given by

$$W_M(\lambda, x, y) = \sum_{T \subseteq E} p(M.T; \lambda) x^{|E - T|} y^{|T|} = \sum_{i=0}^{n} A_M(i, \lambda) x^{n-i} y^i,$$

where $A_M(i, \lambda) = \sum_{T \in \binom{\mathcal{B}}{i}} p(M.T; \lambda)$. Then we proved the following MacWilliams type identity in [2].

**Theorem 3.1** If $M$ is a matroid on the set $E$, then

$$\lambda^{\rho(M)} W_M^*(\lambda, x, y) = W_M(\lambda, x + (\lambda - 1)y, x - y),$$

and for $i = 0, 1, \ldots, n$,

$$\lambda^{\rho(M)} A_M^*(i, \lambda) = \sum_{j=0}^{n} A_M(j, \lambda) \sum_{\nu=0}^{i} (-1)^\nu (\lambda - 1)^{i-\nu} \binom{j}{\nu} \binom{n-j}{i-\nu}.$$

Let $\mathbb{F}$ be a (not necessarily finite) field, and let $\mathbb{F}[z]$ denote the ring of polynomials in an indeterminate $z$ with coefficients in $\mathbb{F}$. Furthermore, define $\mathbb{G} := \mathbb{F}[z] - \{0, 1\}$. For a matroid $M$ on $E$ with at least one cocircuit, we define the following sets:

- $\mathcal{R}_M^\lambda = \{ i \in \{1, \ldots, n-t\} : A_M^*(i, \lambda) \neq 0 \}$;
- $d_M = \min\{|X| : X \text{ is a cocircuit in } M\}$;
- $\mathcal{C}_{M,i} = \{X : X \text{ is a cocircuit of } M \text{ with } |X| = i\}$;
- $\mathcal{H}_{M,i} = \{X : X \text{ is a hyperplane of } M \text{ with } |X| = i\}$;
- $e_M = \max\{ i : \text{ no subset } X \in \binom{E}{i} \text{ contains two distinct cocircuits of } M \}$.

Using the above theorem, we have a generalization of the Assmus-Mattson theorem for matroids.

**Theorem 3.2** Let $M$ be a matroid on $E$ with at least one circuit and one cocircuit, and suppose that $t$ $(0 < t < d_M)$ is an integer with $|\mathcal{R}_M^\lambda| \leq d_M - t$ for some $\lambda \in \mathbb{G}$ such that

1. for all $T \in \binom{E}{i}$ and $l = 1, \ldots, n-t$, $A_{M^*}(l, \lambda) = 0$ whenever $A_{M^*}(l, \lambda) = 0$. 
Then for $m = \min\{e_{M^*}, n-t\}$, $C_{M, d_{M}}$, $C_{M^{2}, d_{M^{*}}}$, $C_{M^{*}, m}$, $H_{M, n-e_{M}}$, $H_{M^{*}, n-m}$, each forms a $t$-design.

Example 3.3 The binary affine matroid $M = AG(3, 2)$, represented by the binary matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
\end{pmatrix},
\]
has minimal cocircuit size $d_{M} = 4$, and the characteristic enumerator of $M^{*}$ (and of $M$) is
\[
W_{M^{*}}(\lambda, x, y) = (\lambda - 1)(\lambda^{3} - 7\lambda^{2} + 21\lambda - 21)y^{8} + 8(\lambda - 1)(\lambda - 4)xy^{7} + 28(\lambda - 1)(\lambda - 2)(\lambda - 4)xy^{6} + 14(\lambda - 1)x^{4}y^{4} + x^{8}.
\]
so $|R_{M,3}| = |\{4\}| = 1 \leq d_{M} - 3$. By letting $\lambda$ be an indeterminate (resp., by setting $\lambda := 2$), Condition 1 in Theorem 3.2 is satisfied for $\lambda$ and $t = 3$. Hence, $C_{M,4}$ and $H_{M,4}$ each form a 3-design.

Let $C$ be an $[n, k]$ code over $\mathbb{F}_{q}$. Let $r, i$ be integers with $1 \leq r \leq k$ and $1 \leq i \leq n$, and define
\[
D_{r}(C) \quad = \quad \{D \ : \ D \text{ is an } r\text{-dimensional subcode of } C\};
\]
\[
S_{r}(C) \quad = \quad \{\text{Supp}(D) \ : \ D \in D_{r}(C)\};
\]
\[
S_{r,i}(C) \quad = \quad \{X \in S_{r}(C) \ : \ |X| = i\};
\]
\[
d_{r}(C) \quad = \quad d_{r} = \min\{|X| \ : \ X \in S_{r}(C)\}.
\]
For an $r$ with $1 \leq r \leq k$, the $r$-th support weight enumerator $A_{C}^{(r)}(x, y)$ of $C$ is defined as follows:
\[
A_{C}^{(r)}(x, y) = \sum_{i=0}^{n} A_{i}^{(r)} x^{n-i} y^{i},
\]
where
\[
A_{i}^{(r)} = A_{i}^{(r)}(C) = |\{D \ : \ \text{Supp}(D) \in S_{r,i}(C)\}|.
\]
Using Theorem 3.1 and Theorem 3.2, we have the Assmus-Mattson type theorem for subcode supports of linear codes.

Theorem 3.4 Let $C$ be an $[n, k, d]$ code over $\mathbb{F}_{q}$ and let $m$ be an integer with $1 \leq m \leq \min\{k, n-k\}$. Suppose that $t$ ($0 < t < d$) is an integer with
\[
|\{i \in \{d_{m}^{\perp}, \ldots, n-t\} \ : \ A_{M^{*}}(i, q^{m}) \neq 0\}| \leq d_{m} - t.
\]
If each $S_{r,i}(C)$ form $t$-designs and $|S_{r,i}(C)| = A_{i}^{(r)}(C)$ whenever $A_{i}^{(r)}(C) \neq 0$, for all $r$ $(1 \leq r \leq m - 1)$ and all $i$ $(d_{r} \leq i < d_{m+1})$, then each $S_{m,i}(C)$ $(d_{m} \leq i < d_{m+1})$ forms a $t$-design. Moreover, if each $S_{r,j}(C^\perp)$ form $t$-designs and $|S_{r,j}(C^\perp)| = A_{j}^{(r)}(C^\perp)$ whenever $A_{j}^{(r)}(C^\perp) \neq 0$, for all $r$ $(1 \leq r \leq m - 1)$ and all $j$ $(d_{r}^\perp \leq j < d_{m+1}^\perp)$, then each $S_{m,j}(C^\perp)$ $(d_{m}^\perp \leq j < d_{m+1}^\perp)$ forms a $t$-design.

From this theorem, we have the following result for doubly-even self-dual codes of length 24, 32 and 48.

**Corollary 3.5** For $n = 24$, 32 or 48, let $C$ be a binary doubly-even self-dual $[n, n/2, 4 \lfloor n/24 \rfloor + 4]$ code. then each $S_{m,i}(C)$ forms a $t$-design as follows:

<table>
<thead>
<tr>
<th>length</th>
<th>$m$</th>
<th>support weights $i$</th>
<th>$t$-designs</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>2</td>
<td>12</td>
<td>5-(24, 12, 660)</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>14</td>
<td>5-(24, 14, 8008)</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>16</td>
<td>5-(24, 16, 65598)*</td>
</tr>
<tr>
<td>24</td>
<td>3</td>
<td>14</td>
<td>5-(24, 14, 4290)</td>
</tr>
<tr>
<td>24</td>
<td>3</td>
<td>15</td>
<td>5-(24, 15, 40040)*</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>12</td>
<td>3-(32, 12, 385)</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>14</td>
<td>3-(32, 14, 10192)</td>
</tr>
<tr>
<td>48</td>
<td>2</td>
<td>18</td>
<td>5-(48, 18, 13328)</td>
</tr>
<tr>
<td>48</td>
<td>2</td>
<td>20</td>
<td>5-(48, 20, 581400)</td>
</tr>
<tr>
<td>48</td>
<td>2</td>
<td>22</td>
<td>5-(48, 22, 15853068)</td>
</tr>
</tbody>
</table>

*by computer search

**References**


