Hyperplanes and hamiltonian circuits in Perfect Matroid Designs with fixed basis

Wojciech Kordecki
University of Business in Wrocław

May 15, 2013

Abstract

We study the number of hamiltonian circuits, containing a fixed basis, and the number of hyperplanes, which do not contain a fixed basis in perfect matroid designs. Projective and affine finite geometries are considered as examples of such matroids. We give algorithms to find the hyperplanes and the hamiltonian circuits in such cases.

1 Introduction

In this note we use a standard matroid terminology – see [6] and [7]. Let \(M = (E, \mathcal{F})\) denote a matroid on a finite nonempty set \(E\), where \(\mathcal{F}\) denotes a family of flats. By \(\rho(A)\) we denote a rank of a set \(A\). A family of circuits is denoted by \(\mathcal{C}\), a family of bases is denoted by \(\mathcal{B}\), and \(\sigma(A)\) denote a span of \(A\). A flat of rank \(\rho(E) - 1\) is called a hyperplane.

We also need some definitions from the theory of projective and affine finite geometries. The monograph of Hirschfeld [4] (see also [1]) gives a detailed and self-contained exposition of finite projective geometries.

Let \(GF(q)\) be a Galois field, where \(q\) is a prime power and let \(V(r, q)\) be an \(r\)-dimensional vector space on \(GF(q)\). By \(\mathcal{L}_P\) we denote the lattice of subspaces of \(V\). Atoms of \(\mathcal{L}_P\) constitute the points of projective geometry \(PG(r - 1, q)\) of dimension \(r - 1\). Let \(e\) be an element of the lattice \(\mathcal{L}_P\). If \(e\) is a subspace of dimension \(k - 1\) and \(k > 2\) we define subspace of rank \(k\) of \(PG(r - 1, q)\) as a set \(A\) of all points \(p < e\), then \(\rho(A) = k\). Recall
that the subspaces of $PG(r - 1, q)$ form a modular geometric lattice, hence if $A, B \in J$, then $\rho(A \cup B) = \rho(A) + \rho(B) - \rho(A \cap B)$, (see Welsh [7], p. 195).

The affine geometry $AG(r - 1, q)$ is obtained from $PG(r - 1, q)$ by deleting from the latter all points of a hyperplane. A line is a subspace of rank 2 and for $x \neq y$, denote $l = L(x, y) = \sigma(\{x, y\})$. Note that every 2-element set is independent.

Let $[x] = q^x - 1$.

Gaussian coefficients are defined as

$$[x] = \prod_{j=1}^{k} \frac{q^{x-j+1} - 1}{q^j - 1} \text{ for } 0 \leq k \leq x.$$ 

It is well known that $PG(r - 1, q)$ and $AG(r - 1, q)$ are matroids $(E, F)$ where $E$ is the set of points of the geometry and $F$ is the family of its subspaces. It is also well known that the ground set $E$ of $PG(r - 1, q)$ has $[r]$ elements, $[r]$ hyperplanes and $[r][r-1]$ subspaces of rank $k$. Similarly, $AG(r - 1, q)$ has $q^{-1}$ elements, $q^{-k}[r-1][r-1]$ subspaces of rank $k$ and $q[r-1]$ hyperplanes.

Let $S_1$ and $S_2$ are subspaces of $PG(r - 1, q)$. By $S_1 \cup S_2 = \sigma(S_1, S_2)$ we denote the smallest subspace containing both $S_1$ and $S_2$. Let $B = \{x_1, \ldots, x_r\}$ be any basis of $PG(r - 1, q)$ and let $H_\alpha$ be a hyperplane.

Kelly and Oxley give ([5], Lemma D), the following result.

**Proposition 1.** If $B$ is a basis of $PG(r - 1, q)$, then there are precisely $(q-1)^{r-1}$ points $p$ of $PG(r - 1, q)$ such that $B \cup \{p\}$ is a circuits.

The following version of Proposition 1 for $AG(r - 1, q)$ is given by Oxley in [6], (Lemma 6.2.4, p. 172).

**Proposition 2.** If $B$ is a basis of $AG(r - 1, q)$ then there are precisely $q^{1}((q - 1)^{r} - (-1)^{r})$ points $p$ of $AG(r - 1, q)$ such that $B \cup \{p\}$ is a circuits.

## 2 Results

In this section we generalise Propositions 1 and 2 to the class of symmetric Perfect Matroid Designs, which includes projective and affine geometries as particular cases.
A perfect matroid design or PMD is a matroid $M$ in which $k$-flat has a common cardinal $\alpha_k$, $1 \leq k \leq \rho(M)$. Such objects were first studied by Young, Murthy and Edmonds in [8], (see Welsh [7], p. 209 and Cameron and Deza [2], Chapter VII.10).

Let $M$ be a matroid of rank $r$, such that following conditions hold:

(i) all flats of the rank $j$ in $M$, $j < r$ are isomorphic,

(ii) the number of flats of rank $s$ in $M$ which contain a fixed flat $M'$ of rank $u$ is equal $f(r, s, u)$ and does not depend on selection of $M'$.

Call a matroid $M$ if it fulfills the above conditions, Symmetric Perfect Matroid Design. We denote it briefly by SPMD. Note, that both $PG(r - 1, q)$ and $AG(r - 1, q)$ are SPMD.

Let $\langle r \rangle_k$ denote the number of flats of rank $k$ (Whitney numbers of the second kind) in a SPMD $M$ of rank $r$. Let $\langle k \rangle = \langle k \rangle_1$, denote the number of elements of such $M$. Consider the number $f(r, s, u)$ of flats of rank $s$ which contains a fixed flat of rank $u$. From the obvious equality

$$\langle r \rangle_s \langle s \rangle_u = \langle r \rangle_u f(r, s, u)$$

we obtain the following formula:

$$f(r, s, u) = \frac{\langle r \rangle_s \langle s \rangle_u}{\langle r \rangle_u}.$$  (1)

If $M$ is $PG(r - 1, q)$ or $AG(r - 1, q)$ and $u > 0$, then from (1) we get

$$f(r, s, u) = \binom{r - u}{s - u}$$

and for $AG(r - 1, q)$ we have

$$f(r, s, 0) = q^{r-s} \binom{r - 1}{s - 1}.$$  

**Theorem 1.** If $B$ is a basis of SPMD $M$ of rank $r$, then there are precisely

$$n = \sum_{k=0}^{r-1} (-1)^k \binom{r}{k} \frac{\langle r \rangle_k \langle r-1 \rangle_k}{\langle k \rangle}$$

hyperplanes $H$ which contain no elements of $B$.  

3
Proof. There are \((r - 1)\) hyperplanes altogether \(rf(r, r - 1, 1)\) among them contain at least one element from \(B\), \(\binom{r}{2}f(r, r - 1, 2)\) contain at least one pair of elements from \(B\), and so on. Hence from the inclusion-exclusion principle we get

\[
n = \sum_{k=0}^{r-1} (-1)^k \binom{r}{k} f(r, r - 1, k).
\]

Hence, from (1), we obtain the assertion. \(\square\)

**Theorem 2.** If \(B\) is a basis of SPMD \(M\) of rank \(r\) then there are precisely

\[
n = \sum_{k=0}^{r} (-1)^{r-k} \binom{r}{k} (\langle k \rangle - k)\]

(3)

elements \(e\) such that \(B \cup e\) is a circuit.

Proof. There are \(\binom{r}{k} (\langle k \rangle - k)\) circuits, containing at most \(k\) elements from the basis \(B\). Since \(\langle 1 \rangle = 1\) and \(\langle 0 \rangle = 0\), we obtain the assertion. \(\square\)

From Theorem 2 we immediately obtain the following result.

**Corollary 1.** If \(B\) is a basis of \(PG(r-1, q)\), then there are precisely \((q-1)^{r-1}\) hyperplanes \(H\) which do not contain any element of \(B\).

Proof. For \(PG(r-1, q)\) or \(AG(r-1, q)\) we have

\[
n = \sum_{k=0}^{r-1} (-1)^k \binom{r}{k} \frac{q^{r-k} - 1}{q - 1} = \frac{1}{q - 1} \left( \sum_{k=0}^{r-1} (-1)^k \binom{r}{k} q^{r-k} - \sum_{k=0}^{r-1} (-1)^k \binom{r}{k} \right)
\]

(4)

Hence, from (4), the assertion follows. \(\square\)

Note, that Proposition 1 and Corollary 1 are strictly related. “Principle of duality” (see Hirschfeld [4]) establishes the one-to-one correspondence between points and hyperplanes – \(p \leftrightarrow H\) and \(p_1 \lor p_2 \leftrightarrow H_1 \cap H_2\).

Since \(AG(r-1, q)\) is a SPMD matroid, then from Theorem 1 we have the following result.
Corollary 2. If $B$ is a basis of $AG(r - 1, q)$, then there are precisely $n = (q - 1)^{r-1} - 1$ hyperplanes $H$ which contain no elements of $B$.

Proof. From (1) it follows that $PG(r - 1, q)$ contains at least one hyperplane which does not contain any element of $B$, (and it contains exactly one if $q = 2$). $AG(r - 1, q)$ has the one such hyperplane less than $PG(r - 1, q)$ has, which establishes the formula. \hfill \Box

Arguing as above, from Theorem 2 one can obtain Propositions 1 and 2 as well. The proofs are similar to the proof of Proposition 1. Note, that the proof of Proposition 2 given in [6] is algebraic in nature, while proof of our more general Theorem 2 has a simple combinatorial form.

3 Algorithms for $PG(r - 1, q)$ and $AG(r - 1, q)$

Until now all known geometric PMD are free matroids, $PG(r - 1, q)$, $AG(r - 1, q)$, Steiner system $S(t, k, v)$ and triffids of typ $(1, 3, 9, 3^n)$ (see Deza [3]). In this section we consider the cases of $PG(r - 1, q)$ and $AG(r - 1, q)$ (which seem the most interesting) in detail. The following two algorithms give constructive methods to obtain hyperplanes described in Corollary 1 and points described in Proposition 1 in the case of $PG(r - 1, q)$.

Algorithm 1.

Input: Basis $B = \{x_1, \ldots, x_r\}$ of $PG(r - 1, q)$.

Output: A family of all hyperplanes $\{H_\alpha\}$ in $PG(r - 1, q)$ such that $\forall \alpha : H_\alpha \cap B = \emptyset$.

1. Let $(x'_1, \ldots, x'_r)$ be an arbitrary permutation of $B$.
2. Let $l_i = L(x'_i, x'_{i+1})$, $1 \leq i \leq r - 1$.
3. Choose $a_i = (y_{i,1}, \ldots, y_{i,q-1})$, an arbitrary sequence of points lying on $l_i$ different from $x'_i$ and $x'_{i+1}$, $1 \leq i \leq r - 1$.
4. Choose $\alpha = (m_1, \ldots, m_{r-1})$, an arbitrary sequence such that $1 \leq m_i \leq q - 1$. There are $(q - 1)^{r-1}$ of such sequences.
5. Let $I_\alpha = \{y_{1,m_1}, \ldots, y_{r-1,m_{r-1}}\}$. The set $I_\alpha$ is independent.
6. Return $H_\alpha = \sigma(I_\alpha) = y_{1,m_1} \lor \cdots \lor y_{r-1,m_{r-1}}$.
Proof. Since \( y_{i,m} \in L(x'_i, x'_{i+1}) \), we have

\[
\{y_{1,m_1}, \ldots, y_{k,m_k}\} \subset \{x'_1, \ldots, x'_k\}
\]

for \( 1 \leq k \leq r - 1 \). Hence \( y_{k,m_k} \notin y_{1,m_1} \lor \cdots \lor y_{k,m_k} \) for every \( k \leq r - 1 \).

Next we have to prove that for every \( i \), \( x'_i \notin H_\alpha \). Suppose, that it is not the case, i.e. there exists \( x'_i \in H_\alpha \). Since from step 3 and step 5 there exists \( y \in L(x'_i, x'_{i+1}) \) (or \( y \in L(x'_i, x'_{i-1}) \)) and therefore \( x'_{i+1} \in H_\alpha \) (or \( x'_{i-1} \in H_\alpha \)). Hence all \( x'_i \in H_\alpha \), while we must have \( \rho(H_\alpha) = r - 1 \).

Algorithm 2.

**Input:** Basis \( B = \{x_1, \ldots, x_r\} \) of \( PG(r - 1, q) \).

**Output:** A family of all points \( \{p_\alpha\} \) such that \( \forall_\alpha : B \lor \{p_\alpha\} \) is a circuit in \( PG(r - 1, q) \).

1. Let \( (x'_1, \ldots, x'_r) \) be an arbitrary permutation of \( B \).
2. Let \( H'_i = \sigma(B \setminus x_i) \).
3. Choose \( b_i = (H''_{i,1}, \ldots, H''_{i,q-1}) \), an arbitrary sequence of \( q - 1 \) hyperplanes, such that \( H'_i \cap H'_{i+1} \subset H''_{i,j} \) different from \( H'_i \) and \( H'_{i+1} \), \( 1 \leq i \leq r - 1 \).
4. Choose \( \alpha = (m_1, \ldots, m_{r-1}) \), an arbitrary sequence such that \( 1 \leq m_i \leq q - 1 \). There are \((q - 1)^{r-1}\) of such sequences.
5. Let \( p_\alpha = H''_{1,m_1} \cap \cdots \cap H''_{r-1,m_{r-1}} \).
6. Return \( p_\alpha \).

Proof. By the “principle of duality” and on the same way as in the proof of Algorithm 1 we obtain the assertion. \( \square \)

From both algorithms we can obtain the following important conclusion. The families \( \{H_\alpha\} \) and \( \{p_\alpha\} \) produced by Algorithm 1 or Algorithm 2 does not depend on the order of points selection at the each step of algorithms.

Similar algorithms for \( AG(r - 1, q) \) can be constructed by a straightforward modification of Algorithms 1 and 2. Since \( AG(r - 1, q) \) is obtained from \( PG(r - 1, q) \) by deletion of a hyperplane, then we add a hyperplane to \( AG(r - 1, q) \) as a step 0. Next, after performing modified the last step 6, the hyperplane \( H_0 \) will be removed.
Algorithm 3.
Input: Basis $B = \{x_1, \ldots, x_r\}$ of $AG(r-1, q)$.
Output: A family of all hyperplanes $\{H_\alpha\}$ in $AG(r-1, q)$ such that $\forall \alpha : H_\alpha \cap B = \emptyset$.

0. Add $[r-1]$ points, which form a hyperplane $H_0$ in $PG(r-1, q)$.

In the next steps, the $PG(r-1, q)$ arisen from $AG(r-1, q)$, is considered. Steps 1 – 5 are the same as in Algorithm 7.

6. If $H_\alpha \neq H_0$, then return $H_\alpha = \sigma (I_\alpha) \setminus H_0$

Algorithm 4.
Input: Basis $B = \{x_1, \ldots, x_r\}$ of $AG(r-1, q)$.
Output: A family of all points $\{p_\alpha\}$ such that $\forall \alpha : B \cup \{p_\alpha\} is a circuit in AG(r-1, q)$.

0. Add $[r-1]$ points, which form a hyperplane $H_0$ in $PG(r-1, q)$.

In the next steps, the $PG(r-1, q)$ arisen from $AG(r-1, q)$ is considered. Steps 1 – 5 are the same as in Algorithm 2.

6. If $p_\alpha \notin H_0$, then return $p_\alpha$.

References

[1] L. M. Batten. Combinatorics of finite geometries. Cambridge University Press, Cambridge, 1997.

[2] P. J. Cameron and M. Deza. Designs and matroids. In C. J. Colbourn and J. H. Dinitz, editors, Handbook of Combinatorial Designs, pages 847–852. Chapman and Hall, Boca Raton, 2007.

[3] M. Deza. Some problems, I care most. European J. Combin, 31:649–675, 2010.

[4] J. W. P. Hirschfeld. Projective Geometries over Finite Fields. Clarendon Press, Oxford, 1998.

[5] D. G. Kelly and J. G. Oxley. Asymptotic properties of random subsets of projective spaces. Math. Proc. Cambridge Phil. Soc., 91:119–130, 1982.
[6] J. G. Oxley. *Matroid Theory*. Oxford University Press, Oxford, 2 edition, 2011.

[7] D. J. A. Welsh. *Matroid Theory*. Academic Press, London, 1976.

[8] P. Young, U. S. R. Murthy, and J. Edmonds. Equicardinal matroids and matroid designs. In *Combinatorial Mathematics and Its Applications*, pages 498–542. University of North Carolina, Chapel Hill, North Carolina, 1970.

Wojciech Kordecki
University of Business in Wrocław
ul. Ostrowskiego 22
53-238 Wrocław
e-mail: wojciech.kordecki@handlowa.eu