The CRC Handbook of Combinatorial Designs

Edited by

Charles J. Colbourn

Department of Computer Science and Engineering
Arizona State University

Jeffrey H. Dinitz

Department of Mathematics and Statistics
University of Vermont

AUTHOR PREPARATION VERSION
25 July 2006

1 Designs and matroids

Peter J. Cameron and M. Deza

1.1 Matroids

1.1 Definition A *matroid* is a pair $(E, \mathcal{I})$, where E is a set and $\mathcal{I}$ a non-empty family of subsets of E (called *independent sets*) satisfying the conditions

- if $I \in \mathcal{I}$ and $J \subseteq I$, the $J \in \mathcal{I}$;
- (the *Exchange Axiom*) if $I_1, I_2 \in \mathcal{I}$ and $|I_2| > |I_1|$, then there exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

1.2 Example

- E is the edge set of a graph G; a set of edges is independent if and only if it is a forest. (Such a matroid is a *graphic matroid*.)
- E is a set of vectors in a vector space V; a set of vectors is independent if and only if it is linear independent. (Such a matroid is a *vector matroid*.)
- E is a set with a family $(\mathcal{A} = (A_i : i \in I)$ of subsets; a subset of E is independent if and only if it is a partial transversal of $\mathcal{A}$. (Such a matroid is a *transversal matroid*.)

1.3 Definition In a matroid $M = (E, \mathcal{I})$,

- a *basis* is a maximal element of $\mathcal{I}$;
- a *circuit* is a minimal element of $\mathcal{P}(E) \setminus \mathcal{I}$;
- the *rank* $\rho(A)$ of a subset A of E is the maximum cardinality of a member of $\mathcal{I}$ contained in A;
- a *flat* is a subset F of E with the property that, for any $e \in E$, $\rho(F \cup \{e\}) = \rho(F)$ implies $e \in F$;
- a *hyperplane* H is a maximal proper flat of M (a flat satisfying $\rho(H) = \rho(E) - 1$).

1.4 Remark

- The Exchange Axiom shows that all bases of a matroid have the same cardinality; more generally, all maximal independent subsets of A have rank $\rho(A)$.
- Matroids can also be defined and axiomatised in terms of their bases, circuits, rank function, flats, or hyperplanes.
- The set of flats of a matroid is closed under intersection. Also, if F is a flat and x a point not in F, then there is a flat F' with $F \cup \{x\} \in F'$ and $\rho(F') = \rho(F) + 1$.

1.5 Definition A *loop* in a matroid M is an element e such that $\{e\} \notin \mathcal{I}$. Two non-loops e_1, e_2 are *parallel* if $\{e_1, e_2 \notin \mathcal{I}$. A matroid is *geometric* if it has no loops and no pairs of parallel elements. A geometric matroid is also called a *combinatorial geometry*

1.6 Remark From any matroid M, we obtain a geometric matroid (the *geometrisation* of M) by deleting loops and identifying parallel elements. The geometrisation of a vector space is the corresponding projective space.

1.7 **Definition** The *truncation* of $M = (E, \mathcal{I})$ to rank r is the matroid on E whose family of independent sets is $\{I \in \mathcal{I} : |I| \leq r\}$. Its flats are the flats of M of rank less than r, together with E.

1.8 **Example** The *free matroid* F_n of rank n is the matroid with $|E| = n$ and $\mathcal{I} = \mathcal{P}(E)$. Its truncation to rank r is the *uniform matroid* $U_{n,r}$.

1.9 **Remark** For more information on matroids, see Oxley [Ox92] or Welsh [We76].

1.2 Perfect matroid designs

1.10 **Definition** A *perfect matroid design*, or *PMD*, is a matroid M, of rank r say, for which there exist integers $f_0, f_1, \ldots, f_r$ such that, for $0 \leq i \leq r$, any flat of rank i has cardinality f_i. The tuple $(f_0, f_1, \ldots, f_r)$ is the *type* of M.

1.11 **Remark** If M is a PMD of type $(f_0, f_i, \ldots, f_r)$, then the geometrisation of M is a PMD of type $(f'_0, f'_1, \ldots, f'_r)$, where $f'_i = (f_i - f_0)/(f_1 - f_0)$. In particular, $f'_0 = 0$, $f_1 = 1$.

1.12 **Theorem** If there exists a PMD of type $(0, 1, f_2, \ldots, f_r)$, then

1. $\displaystyle\prod_{i \leq k \leq j-1} \frac{f_l - f_k}{f_j - f_k}$ is a non-negative integer for $0 \leq i < j \leq l \leq r$;
2. $f_i - f_{i-1}$ divides $f_{i+1} - f_i$ for $2 \leq i \leq r - 1$;
3. $(f_i - f_{i-1})^2 \leq (f_{i+1} - f_i)(f_{i-1} - f_{i-2})$ for $1 \leq i \leq r - 1$.

1.13 **Remark** The above necessary conditions are not sufficient; for example (R. M. Wilson), no PMD of type $(0, 1, 3, 7, 43)$ or $(0, 1, 3, 19, 307)$ exists.

1.14 **Example** Not many PMDs are known. All known geometric PMDs are truncations of examples on the following list:

- Free matroids, with $f_i = i$ for all i.
- Finite projective spaces over a field $\mathbb{F}_q$, with $f_i = (q^i - 1)/(q - 1)$.
- Finite affine spaces: the points are the vectors in a vector space of rank r over $\mathbb{F}_q$; the independent sets are those which are affine independent. (The set $\{v_1, \ldots, v_k\}$ is *affine independent* if $\{v_2 - v_1, \ldots, v_k - v_1\}$ is linearly independent.) These have $f_i = q^i$.
- Steiner systems. (Given a Steiner system $S(t, k, v)$ on the set E, we take the independent sets to be all sets of cardinality at most t together with all $(t+1)$-sets not contained in a block. Then the hyperplanes are the blocks of S.) Note that these PMDs have rank $t + 1$ and are characterised by the property that $f_i = i$ for $i < t$; we have $f_t = k$ and $f_{t+1} = v$.
- Hall triple systems (see below): these have rank 4, $f_2 = 3$, and $f_3 = 9$, and the number of points $|E|$ is a power of 3.

1.15 **Remark** A *line*, resp. *plane* in a PMD is a flat of rank 2, resp. 3. The points and lines of a geometric PMD form a Steiner system $S(2, f_2, f_r)$; the flats form subsystems, so that (for example) any three non-collinear points lie in a unique plane.

1.16 **Theorem** Let M be a geometric PMD of rank 4.

- If the planes in M are projective planes (that is, if $f_3 = f_2^2 - f_2 + 1$ with $f_2 > 2$), then M is a truncation of a projective space.

- If the planes in M are affine planes (that is, if $f_3 = f_2^2$), and if $f_2 > 3$, then M is a truncation of an affine space.

1.17 **Remark** There is a wide gap between the restrictions imposed by Theorem 1.12 and the known examples. For example, it is not known whether there is a PMD of type $(0, 1, 3, 13, 183)$, $(0, 1, 3, 13, 313)$, or $(0, 1, 3, 15, 183)$.

1.3 Hall triple systems and their algebraic siblings

1.18 **Remark** Call a *triffid* any PMD of rank 4 with type $(0, 1, 3, 9, 3^n)$. There is an equivalence between those PMDs and each of following structures:

1. *Hall triple system*, i.e. Steiner triple system $S(2, 3, 3^n)$ on E, $|E| = 3^n$, such that for any point $a \in E$ there exist an involution which has a as unique fixed point.
2. *Finite exponent 3 commutative Moufang loop* (*exp3-CML*, for short), i.e. a finite commutative loop $(L, \cdot)$, such that for any $x, y, z \in L$, $(x \cdot x)c(x \cdot z) = (x \cdot y) \cdot (x \cdot z)$ and $(x \cdot x) \cdot x = 1$ hold.
3. *Distributive Manin quasigroup*, i.e. a groupoid $(Q, \circ)$, such that for any $x, y, z \in Q$, $x \circ y = y \circ x$ and $x \circ (x \circ y) = y$ (i.e, any relation $x \circ y = z$ is preserved under permutation of the variables; in particular, $(Q, \circ)$ is a quasigroup) and all translations are automorphisms.
4. *Restricted Fischer pair* (G, F), i.e. a group G generated by a subset F, such that $x^2 = 1 = (xy)^3$ and $xyx \in F$ for any $x, y \in F$ and such that the commutative center of G is just $\{1\}$.

1.19 **Remark** A triffid is a truncation of an affine space over $\mathbb{F}_3$ if and only if corresponding exp3-CML is a group; then the group is Z_3^n. The first (and smallest) example of a non-associative exp3-CML was given in 1937 by Zassenhaus, by defining, on the set of all 81 $(0, 1, 2)$-sequences $x = (x_1, x_2, x_3, x_4)$, the product as

$$x \cdot y = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4 + (x_3 - y_3)(x_1 y_2 - x_2 y_1))$$

(all above sums are modulo 3).

The number of non-associative exp3-CMLs of order 3^n is $1, 1, 3, 12, > 41$ for $n = 4, 5, 6, 7, 8$, respectively.

1.20 **Remark** The *dimension* $d(L)$ of a exp3-CML L is the smallest number m such that there exist a $(m + 1)$-set generating it; it is usual dimension of corresponding Steiner triple system. Denote by L_m the *free* exp3-CML of dimension m, i.e. such that any exp3-CML of dimension m is its homeomorhic image. One has $|L_m| = 3^4$, 3^{12}, 3^{49}, 3^{220}, 3^{1028}, 3^{4592} for $m = 3, 4, 5, 6, 7, 8$ (Smith [Sm82]). Moreover, $d(L) \leq \log_3 |L|$, with equality only if L is associative, i.e. an Abelian 3-group. The number of exp3-CMLs L with $|L| = 3^n$ and $d(L) = 4$ is $1, 1, 1, 1, 4$ for $n = 4, 5, 6, 7, 8$ (Bénéteau [Be80]).

1.21 **Remark** The associative center $Z(L)$ of a exp3-CML L is the Abelian 3-group $\{z \in L : (x \cdot y) \cdot z = x \cdot (y \cdot z)\}$. The *central quotient* $L^{(1)} = L/Z(L)$ is again a exp3-CML; define $L^{(i)}$ as $L^{(i-1)}/Z(L^{(i-1)})$. The *nilpotency class* $k(L)$ of L is the smallest number k such that $L^{(k)}$ is associative. Then $k(L) \leq d(L)$, with equality for the free loop L_m. All exp3-CML's L with $k(L) = 2$ are classified in [KeNe81] and [RoRC84].

1.22 **Remark** Infinite exp3-CMLs were connected by Manin with cubic hypersurfaces; see, for example [Be99] for recent developments. For connections with differential geometry (3-webs) and topological algebra, see, for example, [Na00].

1.4 Designs in PMDs

1.23 Definition Let t, k, v, λ be integers with $0 \le t < k < v$ and $\lambda > 0$. Let M be a PMD of rank v. A t-(v, k, λ) *design in* M is a family $\mathcal{B}$ of k-flats of M with the property that every t-flat in M is contained in exactly λ members of $\mathcal{B}$.

1.24 Remark

- A t-(v, k, λ) design in the free matroid F_v is just a t-(v, k, λ) design in the usual sense.
- A t-(v, k, λ) design in a PMD M is also a s-$(v, k\lambda_s)$ design in M for $s < t$, where

$$\lambda_s = \lambda \cdot \prod_{i=s+1}^{t} \frac{f_v - f_s}{f_k - f_s}.$$

- A t-(v, k, λ) design in a PMD M of type $(f_0, f_1, \ldots, f_v)$ is an ordinary s-design, where $s = \min(t, \max\{i : f_i = i\})$.

Apart (obviously) from ordinary t-designs, the only case to have been studied is that of t-designs in projective spaces over $\mathbb{F}_q$. To simplify the notation, we put $[n]_q = (q^n - 1)/(q - 1)$, so that the projective space has type $([0]_q, [1]_q, \ldots, [v]_q)$; and define the *Gaussian coefficient*

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{[v-i]_q}{[k-i]_q}$$

to be the number of k-flats.

In this case, some theory has been developed (for example, the analogue of the theorem of Ray-Chaudhuri and Wilson holds: in a $2s$-design in M, the number of blocks is at least $\begin{bmatrix} v \\ s \end{bmatrix}_q$. There are also a few known examples:

1.25 Example

- The first examples were due to Thomas [Th73]. They live in $\mathrm{PG}(n, 2)$, where $n+1$ is coprime to 6; blocks are planes, and any line is contained in seven blocks.
- Ray-Chauduhri and Schram [RS94] gave a few more constructions.
- A recent investigation appears in Braun *et al.* [BKL05].

1.26 Remark It is unknown whether the analogue of Teirlinck's Theorem holds: do t-designs (without repeated blocks, and such that not every k-flat is a block) exist for all t?

1.5 Permutation groups

1.27 Definition A *base* in a permutation group G is a sequence of points whose pointwise stabiliser in G is the identity. A base is *irredundant* if no point is fixed by the stabiliser of its predecessors.

In general the bases of a permutation group do not satisfy the matroid basis axioms!

1.28 Definition An *IBIS group* is a permutation group satisfying the following three conditions (shown to be equivalent by Cameron and Fon-Der-Flaass):

- all irredundant bases contain the same number of points;
- the irredundant bases are preserved by reordering;
- the irredundant bases are the bases of a matroid.

The *rank* of an IBIS group is the rank of its associated matroid.

1.29 Definition A permutation group is *base-transitive* if it permutes its ordered bases transitively. Clearly every base-transitive group is an IBIS group; moreover, the associated matroid is a PMD, and we define the *type* of the group to be the type of the PMD. A permutation group is base-transitive if and only if the pointwise stabiliser of any sequence of points is transitive on the points it doesn't fix (if any).

1.30 Remark The base-transitive permutation groups with rank greater than 1 have been classified by Maund [Ma89]: the list is too long to give here. Maund's proof of this theorem used the Classification of Finite Simple Groups (CFSG). An 'elementary' (but by no means easy) determination of base-transitive groups of rank at least 7, not using CFSG, was given by Zil'ber [Zi83]

1.31 Remark A definition of *permutation geometries*, the analogue in the semilattice of subpermutations (partial bijections) of a set, was given by Cameron and Deza. Following the matroid flat axioms they defined a permutation geometry to be a family $\mathcal{F}$ of subpermutations, closed under intersections, and having the property that if $F \in \mathcal{F}$ and x and y are points with x not in the domain, and y not in the range, of F, there is a unique $F' \in \mathcal{F}$ with rank one greater than the rank of F, extending F and mapping x to y.

A *geometric set* of permutations is a set which consists of the maximal elements in a permutation geometry, and a *geometric group* is a geometric set which forms a group. Now a geometric group is the same thing as a base-transitive group.

1.32 Theorem Let G be an IBIS group of rank $r > 1$ whose associated matroid is uniform. Then G is $(r-1)$-transitive (and the stabiliser of any r points is the identity).

1.33 Remark For $r = 2$, the groups in the conclusion of this theorem are precisely the *Frobenius groups*; a lot of information about their structure is known (Frobenius, Zassenhaus, Thompson). For $r = 3$, they are the *Zassenhaus groups*; these have been determined (Zassenhaus, Feit, Ito, Suzuki) without the use of CFSG. For $r > 3$, they were determined by Gorenstein and Hughes. In particular, the only ones with $r \geq 5$ are symmetric and alternating groups and the Mathieu group M_{12}.

1.6 Some generalizations of PMD

1.34 Remark

1. A *matroid design* is a matroid whose hyperplanes form a BIBD, i.e. a (b, v, r, k, λ)-configuration on 1-flats. Any PMD is a MD. Any BIBD is a PMD of rank3 if $\lambda = 1$, but never a MD if $\lambda = 2$. Kantor [Ka69] showed that the point-hyperplanes design of PG(n,q) is unique *symmetric* BIBD with $\lambda > 1$, which is a MD. Welsh [We76] contain some necessary conditions for a BIBD to be a MD and information of *base designs*, i.e. matroids whose bases are the blocks of a BIBD, and *circuit designs*, i.e. matroids whose circuits are the blocks of a BIBD.
2. An *equicardinal matroid* is a matroid, such that all its hyperplanes have the same cardinality k; they are classified for $|E| - k$ being prime or the square of a prime, as well as for the case of rank 3 matroids (Kestenband and Young, 1978).
3. The following notion generalizes all known PMD of rank 4. A *planar M-space* is a combinatorial geometry of rank 4, such that all its restictions on a 3-flat are isomorphic to the given combinatorial geometry M of rank 3. An example

of planar M-space (with at least two 2-flats) having two different 2-flat sizes is known, but only one.

4. Brylawski [Br79] considered *latticially uniform* (or latticially homogeneous) matroids, i.e. such that for all i-flats x, all upper intervals $[x, E]$ (or, respectively, all lower intervals $[\emptyset, x]$), in the lattice of the flats) are equal.
5. PMDs are the extremal case for the families of k-subsets of given v-set intersecting pairwisely in $l_0, l_1 \ldots, l_t$ elements. It was shown in [De78] that for $v > v_0(k)$, such family contains at most $\prod_0 \leq i \leq t \frac{v-l_i}{k-l_i}$ sets with equality if and only if it the hyperplane family of a PMD with type $(l_0, l_1, \ldots, l_t, k, v)$.

References

[Be80] L. Bénéteau, Free commutative Moufang loops ant anticommutative graded rings, *J. Algebra* **67** (1980) 1–35.

[Be99] L. Bénéteau, Extended triple systems: geometric motivations and algebraic constructions, *Discrete Math.* **208/209** (1999) 31–47.

[BKL05] M. Braun, A. Kerber and R. Laue, Systematic Construction of q-Analogs of t-(v, k, λ)-Designs, *Designs, Codes and Cryptography* **34** (2005), 51–66.

[Br79] T. H. Brylawski, Intersection theory for embedding of matriods into uniform geometries, *Stud. Appl. Math.* **61** (1979) 211–244.

[CD79] P. J. Cameron and M. Deza, Permutation Geometries, *J. London Math. Soc.* (2) **20** (1979) 373–386.

[CF95] P. J. Cameron and D. G. Fon-Der-Flaass, Bases for permutation groups and matroids, *Europ. J. Combinatorics* **16** (1995), 537–544.

[De78] M. Deza, Pavage généralise parfait comme généralization de matroide-configurations, in *Problèmes Combinatoires*, Coll. Int. CNRS **260** pp. 97–100, Paris-Orsay.

[De92] M. Deza, Perfect Matroid Designs, in *Matroid Applications* ed. N. White, pp. 54–72, Encyc. Math. Appl. **40**, Cambridge University Press, 1992.

[DS90] Deza-Sabidussi M. Deza and G. Sabidussi, Combinatorial structures arising from commutative Moufang loops, chapter VI in *Quasigroups and Loops: Theory and Applications* ed.O.Chein, H.O.Pflugfelder and J.D.H.Smith, Sigma Series in Pure Mathematics **8**, pp. 151–160, Heldermann, Berlin, 1990.

[Ha60] M. Hall Jr., Authomorphisms of Steiner triple systems, *IBM J. Res. Devel.* **4** (1960) 460–472.

[Ka69] W. M. Kantor, Characterizations of finite projective and affine spaces, *Canad. J. Math.* **21** (1969), 64–75.

[KeNe81] T. Kepka and P. Nemec, Commutative Moufang loops and distributive groupoids of small order, *Czechoslovak. Math. J.* **31 (106)** 633-669.

[KY78] B. C. Kestenband and H. P. Young, Matroid designs of prime power index, *J. Combinatorial Theory* Ser. A **24** (1978), 211–234.

[Ma89] T. C. Maund, D. Phil. thesis, Oxford University, 1989.

[MYE70] U. S. R. Murty, H. P. Young and J. Edmonds, Equicardinal matroids and matroid-designs, in Proc. 2nd Chapel Hill Conference on Combinatorial Structures and Applications, Gordon and Breach, pp. 498–547, New York, 1970.

[Na00] G. P. Nagy, *Algebraic commutative Moufang loops*, PhD Thesis, Math. Institut, Universitat Erlangen-Nurnberg, 2000.

[Ox92] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[RS94] D. K. Ray-Chaudhuri and E. J. Schram, A large set of designs on vector spaces. *J. Number Theory* **47** (1994), 247–272.

[RoRC84] R. Roth and D. K. Ray-Chaudhury, Hall triple systems and commutative Moufang exponent 3 loops: the case of nilpotence class 2, *J. Comb. Theory* Ser. A **36** (1984) 129–162.

[Sm82] J.D.H.Smith, *Commutative Moufang loops and Bessel functions*, Invent. Math. **67** (1982) 173–186.

[Th73] S. Thomas, Designs over finite fields, *Geom. Dedicata* **24** (1987), 237–242.

[We76] D. J. A. Welsh, *Matroid theory*, LMS Monographs **8**, Academic Press, London-New York, 1976.

[Yo73] H. P. Young, *Affine triple systems and matroid designs*, Math. Z. **132** (1973) 343–359; Math.Rev. **50** 142.

[Zi83] B. I. Zil'ber, The structure of models of uncountably categorical theories, pp. 359–368 in *Proc. Internat. Congr. Math.* Vol. 1 (Warsaw 1983).