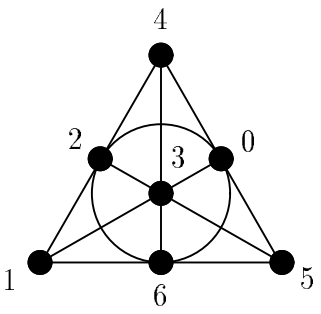
Constructing t-Designs with $t > 3$

Donald L. Kreher
Department of Mathematical Sciences, Michigan Technological University, Houghton MI 49931
kreher@mtu.edu

Extended abstract

A t–(v, k, λ) design is a pair $(X, \mathcal{B})$ where: X is a v–element set of *points*; $\mathcal{B}$ is a family of a family of k-elements subsets of X, called *blocks*; and every t-element subset $T \subseteq X$ is contained in exactly λ blocks. Is is said to be *simple* if all the members of $\mathcal{B}$ are distinct. For example a 2-(7,3,1) design $(X, \mathcal{B})$ is given by:

$X = \{0, 1, 2, 3, 4, 5, 6\}$ and
$\mathcal{B} = \{130, 124, 235, 346, 450, 156, 260\}$



This design is also called the Fano plane. The blocks are easily remembered by the 6 lines and one circle in the adjacent diagram. It is unique up to isomorphism and has the 2-homogeneous group PSL(2,q) generated by $(0, 1, 2, 3, 6, 5, 4)$ and $(1, 2)(3, 6)$ as an automorphism group. Let α be a permutation on X. Then if $x \in X$ we denote the image of x under α by x^α. Furthermore the image of $B \subseteq X$ under α is $B^\alpha = \{x^\alpha : x \in B\}$. A subgroup G of Sym(X), the symmetric group, is an *automorphism group* of the t-design $(X, \mathcal{B})$ if

$$B^\alpha = \{x^\alpha : x \in B\} \in \mathcal{B}$$

for every block $B \in B$ and $\alpha \in G$. If the design has no other automorphisms, then G is said to be the *full automorphism group* In Table I the smallest possible or smallest known t-design is given for $2 \leq t \leq 7$.

Table I: Smallest t-designs

The smallest possible 2-design.

PARAMETERS: 2-(7,3,1) $b = 7$

AUT. GROUP: $PSL_2(7)$ 2-Homogeneous.

GENERATORS: $(0,1,2,3,6,5,4)$, $(1,2)(3,6)$

BASE BLOCK: 013

The smallest possible 3-design.

PARAMETERS: 3-(8,4,1) $b = 14$

AUT. GROUP: $PSL_2(7)$ 3-Homogeneous.

GENERATORS: $(0,1,2,3,4,5,6)(7)$, $(0,7,1)(2,4,6)(3)(5)$.

BASE BLOCK: 0137

The smallest possible 4-design

PARAMETERS: 4-(11,5,1) $b = 66$

AUT. GROUP: M_{11} 4-Homogeneous.

GENERATORS:
$(0,1,2)(3,4,5)(6,7,8)$, $(0)(1,3,2,6)(4,5,8,7)$,
$(0)(1,8,2,4)(3,5,6,7)$, $(0,9)(1)(2)(3,6)(4,5)(7,8)$,
$(0)(1)(2)(3,7)(4,8)(5,6)(9,a)$

BASE BLOCK: 02346

The smallest possible 5-design

PARAMETERS: 5-(12,6,1) $b = 132$

AUT. GROUP: M_{12} 5-Homogeneous.

GENERATORS:
$(0,1,2)(3,4,5)(6,7,8)$, $(0)(1,3,2,6)(4,5,8,7)$,
$(0)(1,8,2,4)(3,5,6,7)$, $(0,b,a,9)(1)(2)(3,8,6,4)(5)(7)$

BASE BLOCK: 012345

The smallest possible 6-design

PARAMETERS: 6-(14,7,4) $b = 1716$

AUT. GROUP: C_{13} Not even transitive.

GENERATORS: $(0,1,2,3,4,5,6,7,8,9,a,b,c)(d)$

BASE BLOCKS:

$013459d$	$014567d$	$012457d$	$012346d$	$012345d$	$012367d$
$023567d$	$034567d$	$024567d$	$012458d$	$023468d$	$012468d$
$012368d$	$012568d$	$012378d$	$014568d$	$034568d$	$013478d$
$023578d$	$024578d$	$012678d$	$024569d$	$012469d$	$023459d$
$014569d$	$014579d$	$012579d$	$012479d$	$023579d$	$013679d$
$012589d$	$024589d$	$034689d$	$013469d$	$035678d$	$01467ad$
$014789d$	$01347ad$	$02368ad$	$02358ad$	$02567ad$	$01458ad$
$01368ad$	$024678d$	$023478d$	$023479d$	$023469d$	$025679d$
$024679d$	$025689d$	$023689d$	$023589d$	$012356d$	$013467d$
$013458d$	$013579d$	$015678d$	$013578d$	$013569d$	$013489d$
0145789	0134567	0123457	0124567	0234568	0123458
0124678	0235678	0234569	0123459	0245678	0124679
0234579	0123679	0125679	0345679	0345689	0124689
0123689	0145689	0125789	0124789	$012457a$	$023457a$
$012367a$	$023467a$	0136789	$023458a$	$012468a$	$023568a$
$012568a$	$012578a$	$014578a$	$013457a$	0236789	0234678
$012569a$	0245689	0234789	$024567a$	0256789	$024568a$
$023478a$	$023569a$	$014678a$	$013479a$	$024579a$	$024679a$
0123479	$013579a$	$012579a$	$013579b$	0134568	0123567
$013568a$	0134578	0123578	0134678	0123489	0134679
0123569	0123589	0135689	0345789	$013567a$	$013468a$
$035679d$	$01247ad$	$035789d$	$034789d$	$036789d$	$02357ad$

The smallest known 7-design

PARAMETERS: 7-(33,8,10) $b = 5,340,060$

AUT. GROUP: $PSL_2(32)$ 4–homogeneous.

GENERATORS:

$(1,2,4,8,g)(3,6,c,o,h)(5,a,k,9,i)(7,e,t,p,j)(b,m,d,q,\ell)(f,v,u,s,n)$, $(1,i,v)(2,\ell,c)(3,a,t)(4,w,x)(5,o,e)(6,7,h)(8,p,s)(9,j,k)(b,f,d)(g,n,u)(m,0,q)$

BASE BLOCKS:

01234568 01235789 $0123569a$ $1234678c$ $0123567a$ $013689ab$
$0124568a$ $0134678b$ 01345789 $1234789a$ $0145678a$

A subgroup G of $\mathrm{Sym}(X)$ is t-Homogeneous on X if the t-element subsets of X fall into a single orbit under G. If G is t-Homogeneous on X, then every orbit of k-element subsets of X is a t–(v,k,λ) design for some λ. The classification of finite simple groups shows that there are no t-homogeneous groups with $t > 5$ other then the alternating and symmetric groups. Consequently, the following statements were heard in the 1980's

Unknown group theorist (≈1980): There will not be any 6-designs.

Cameron & van Lint (1980), [2]: The existence of non-trivial t–designs with $t > 5$ is the most important unsolved problem in the area.

Leavitt & Magliveras (1984), [11]: A 6-(33,8,36) design exist!

Kramer, Leavitt & Magliveras (1985), [5]: A 6-(20,9,112) design exist!

Kreher & Radziszowski (1986), [8]: There exist 6-(14,7,4) designs!

Unknown group theorist (≈1986): O.K. what I meant was that will not be any interesting 6-designs

Cameron & van Lint (1991), [3]: The existence of Steiner systems with large t is possibly the most important open problem in design theory (A t-$(v,k,1)$ design is also called a Steiner system.)

In Table III we see that almost every known t-design with $t > 5$ was constructed by a union of group orbits. Indeed given integers $0 < t < k < v$, v-set X and $G \leq \mathrm{Sym}(X)$ let:

- $\Delta_1, \Delta_2, \ldots, \Delta_{N_t}$ be the orbits of t-subsets;
- $\Gamma_1, \Gamma_2, \ldots, \Gamma_{N_k}$ be the orbits of k-subsets;
- $A_{tk}[\Delta_i, \Gamma_j] = |\{K \in \Gamma_j : K \supseteq T\}$, $T \in \Delta_i$ fixed.

Kramer and Mesner in 1973, [4] observed that a t-(v,k,λ) design exists with $G \leq Sym(X)$ as an automorphism group if and only if there is a (0,1)-solution U to the matrix equation

$$A_{tk}U = \lambda J,$$

where: $J = [1,1,1,\ldots,1]^T$.

For example let $G = \langle (1,4,5)(2,0,6),(2,6)(4,5)\rangle$, then the $A_{2,3}$ matrix is:

	123		125		120					
	340		140		460					
	136		146		160					
	356	124	456	126	256	134	130		236	
	350	450	150	240	250	345	346		230	
	234	156	245	560	246	135	235	145	360	260
$\left\{\begin{matrix}12\ 40\ 16\\56\ 50\ 24\end{matrix}\right\}$	1	1	1	1	1	0	0	0	0	0
{13 34 35}	2	0	0	0	0	2	1	0	0	0
{14 45 15}	0	1	2	0	0	1	0	1	0	0
{10 46 25}	0	0	2	0	2	0	1	0	0	0
{23 30 36}	2	0	0	0	0	0	1	0	2	0
{26 20 60}	0	0	0	1	2	0	0	0	1	1
		↑					↑			↑

A solution to $A_{2,3}U = J$ is $U = [0,1,0,0,0,0,1,0,0,1]^T$. Hence $\mathcal{B} = \left\{\begin{matrix}124\\450\\156\end{matrix}\right\} \bigcup \left\{\begin{matrix}130\\346\\235\end{matrix}\right\} \bigcup \{260\}$ is a 2-(7,3,1) design with G as an automorphism group.

The *method* we use to construct t-designs with $t > 3$ is abstractly the following procedure.

A. Choose parameters t, k, v, and λ;

B. Find a candidate for an automorphism group G;

C. Generate the incidence matrix A_{tk};

D. Solve the system of equations $A_{tk}U = \lambda J$ for one, some or all (0,1)-vectors U;

E. Check for any special properties required of the solutions found;

F. Apply any known recursive methods to the solutions found to construct more designs.

Almost every known 6 & 7-design was either found this way or obtained from a 6 or 7-design found this way. See Table III.

In [7] we argue that it becomes apparent that the techniques used to find t-designs with $t > 3$ are very different from the methods used to find designs with $t \leq 3$. Furthermore, when $t > 5$ the methods and techniques change again. This is partly due the objects and tools that that exist from which the designs can be made. See Table II.

Table II: Available ingredients

$t = 2, 3$	Latin squares, transversal designs, orthogonal arrays of strength 2, rich source of 2 and 3 homogeneous groups, recursive constructions, geometry.
$t = 4, 5$	A few 4 and 5 homogeneous groups, union of orbits under other groups, coding theory.
$t \geq 6$	Union of group orbits,

Table III: The known t-designs, $t \geq 6$.

Parameters	Aut. Group.	Size of A_{tk}	Method
6-(14,7,4)	C_{13}	99 by 132	Basis reduction
• Kreher & Radziszowski 1986, [8]			
6-$(6+8u, 7, 4u)$ $u > 0$	?	?	L.S. recursion
• Teirlinck 1989, [15]			
6-(20,9,112)	$PSL(2,19)$	19 by 52	Leavitt's Alg.
• Kramer, Leavitt & Magliveras 1985, [5]			
6-(22,8,60)	$PSL(2,19)pp$	36 by 120	Basis Reduction
6-(23,8,68)	?	?	Cleverness
6-$(23+16m, 8, \frac{1}{2}\binom{16m+1}{2})$ $m \geq 0$	?	?	L.S. recursion
• Kreher 1993, [6]			
6-$(28, 8, \lambda)$ $\lambda \in \{63, 84, 105\}$	$P\Gamma L(2,27)$	14 by 72	Cleaver backtracking
• Schmalz 1993, [16]			
6-(33,8,36)	$P\Gamma L(2,32)$	13 by 97	Leavitt's Alg.
• Magliveras & Leavitt 1984, [11]			
6-(32,7,10)	?	?	Derived design of 7-(33,8,10)
6-(32,8,125)	?	?	Residual design of 7-(33,8,10)
6-(33,8,135)	?	?	The 7-(33,8,10) as a 6-design
7-(33,8,10)	$P\Gamma L(2,32)$	32 by 97	Basis Reduction
• Betten, Kerber, Kohnert, Lau & Wasserman 1995, [1]			
t-$(v, t+1, \lambda)$ $v \equiv t \pmod{\lambda}$, $\lambda = (t+1!)^{2t+1}$	?	?	magic and L.S. recursion
• Teirlinck 1987, [14]			

The difficulty in the above method is part D. That is in solving

$$A_{tk}U = \lambda J, \tag{1}$$

for $(0,1)$-valued vector U. This equation can be solved by using backtracking if the N_t by N_k dimensions of A_{tk} are small, but becomes impossible when they are larger. For such equations we use alternative methods. The most successful has been *basis reduction* [9].

Observe that if U is a $(0,1)$-solution to equation 1, then U satisfies

$$\begin{bmatrix} I & 0 \\ A_{tk} & -\lambda J \end{bmatrix} \begin{bmatrix} U \\ 1 \end{bmatrix} = \begin{bmatrix} U \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Conversely let $\mathcal{B}$ be the set of columns of

$$\begin{bmatrix} I & 0 \\ A_{tk} & -\lambda J \end{bmatrix}$$

and let $\mathcal{L} = Span(\mathcal{B}) \subset \mathbb{Z}^{n+m}$. Then $\mathcal{L}$ is a $n+m$-dimensional lattice with basis $\mathcal{B}$. Observe that if

$$\begin{bmatrix} U \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathcal{L},$$

where U a $(0,1)$–vector, then $A_{tk}U = m\lambda$ for some integer m. Consequently any $(0,1)$–vector $\mathbf{U} = \begin{bmatrix} U \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathcal{L}$ yields a t–$(v,k,m\lambda)$ design for some integer m.

The key observation is that $\mathbf{U}$ is a short vector of $\mathcal{L}$. More precisely the Euclidean length $||\mathbf{U}|| < \sqrt{N_k}$ and it can be observed

that most of the vectors in any basis of $\mathcal{L}$ that contain $\mathbf{U}$ have length greatly exceeding $\sqrt{N_k}$. Consequently we seek tools to find bases for $\mathcal{L}$ that have vectors of small Euclidean length. Hopefully our desired solution to equation 1 will be among them. The available tools to date are:

1. The L^3 algorithm by Lenstra, Lenstra and Lováz 1982, [10].

2. The improvements by Kreher and Radziszowski 1986, [9].

3. The improvements by Schnor and Euchner 1988/1991, [12, 13].

The following reduced basis algorithm can be found in the 1982 paper of Lenstra, Lenstra, and Lovász, [10] It is often called the L^3 or Lovasz algorithm.

Step 1 Let $\mathcal{B} = [b_1, b_2, \ldots, b_n]$ be a basis for lattice $\mathcal{L}$.

Step 2 Let $\mathcal{B}^* = [b_1^*, b_2^*, \ldots, b_n^*]$ be the Gram–Schmidt orthogonalization of $\mathcal{B}$.

$$\begin{aligned} b_1^* &= b_1; \\ b_2^* &= b_2 - \alpha_{1,2} b_1^*; \\ &\vdots \\ b_j^* &= b_j - \sum_{i=1}^{j-1} \alpha_{ij} b_i^* \\ &\vdots \end{aligned}$$

where $\alpha_{ij} = \dfrac{b_i^* \cdot b_j}{||b_i^*||^2}$ for $i < j$.

Step 3 For $j = 2$ to n

do { For $i = j - 1$ down to 1

do { $b_j \leftarrow b_j - \hat{\alpha}_{ij} b_i$,
where $\hat{\alpha}_{ij}$ is the integer closest to α_{ij}.
recompute α_{ij}.

Step 4 If $||b_{j+1}^* + \alpha_{j,j+1} b_j^*||^2 < \frac{3}{4}||b_j^*||^2$ for some j, interchange b_j and b_{j+1} and return to step 1.

It is shown in [10] that given a basis $\mathcal{B}$ of lattice $\mathcal{L} \in \mathbb{Z}^r$ that the L^3 algorithm produces a *reduced* basis $\mathcal{B}'$ of $\mathcal{L}$, such that:

i. L^3 uses at most $\mathcal{O}(n^4)$ arithmetic operations.

ii. B' is *almost* orthogonal.

iii. $\mathcal{B}'$ contains short vectors. They prove that it contains a vector that is shorter than $2^n \cdot$(length of shortest nonzero vector in $\mathcal{L}$). In practice it has much much better performance.

The simplest form of the basis reduction algorithm to find a solution to

$$AU = R$$

for a $(0,1)$–valued vector U; where A and R are integer valued matrices is the following algorithm:

Step 1	Set $\mathcal{B} = \begin{bmatrix} I & \vec{0} \\ A & -R \end{bmatrix}$, and $\bar{\mathcal{B}} = \begin{bmatrix} I & \vec{0} \\ A & AJ - R \end{bmatrix}$,
Step 2	Consider the lattice $\mathcal{L}(\mathcal{B})$ where $\mathcal{B}$ is the matrix given above.
Step 3	Find a reduced basis $\mathcal{B}'$ of $\mathcal{L}(\mathcal{B})$.
Step 4	Check if $\mathcal{B}'$ contains a column of the form $[\pm U, \vec{0}]$ with $U \in \{0,1\}^n$. If so stop; U solves equation $AU = R$.
Step 5	Repeat Steps 1 to 3 with $\mathcal{B}$ replaced with $\bar{\mathcal{B}}$. If a vector $[\pm U, \vec{0}]$ with $U \in \{0,1\}^n$. is found as column of the new reduced basis, then $J - U$ solves $AU = R$. Otherwise, stop. No solution has been found.

In [9] other basis reduction tools are introduced and the algorithm is modified so that instead of stopping in step 5 it continuously loops back to Step 3 using these other basis reduction tools to reduce the lengths of the vectors in the basis. When either the basis cannot

be reduced any further or a solution is found the algorithm stops. The difficulty with this is that the algorithm may get stuck on bases "surrounding" a local minimum that is not near enough to a solution for the solution to be contained in the basis. Plans to alleviate this condition are being studied.

For further information on combinatorial designs and algorithms that search for them the reader is directed to the soon to be released CRC Handbook of combinatorial designs, in the *CRC* reference series in discrete mathematics. Contact the editors Charles J. Colbourn (`cjcolbou@math.uwaterloo.ca`) and Jeff H. Dinitz (`dinitz@uvm-gen.emba.uvm.edu`) for more information.

References

[1] A. Betten, A. Kerber, A. Kohnert, R. Laue and A. Wasserman, The discovery of simple 7-designs with automorphism group $P\Gamma L(2,32)$, preprint, 1995.

[2] P.J. Cameron and J.H. van Lint, *Graphs, Codes and Designs*, LMS Lecture Note Series **43**, 1980, page 1.

[3] P.J. Cameron and J.H. van Lint, *Designs, Graphs, and their Links*, LMS Student Texts **22**, 1991, page 2.

[4] E.S. Kramer and D.M. Mesner, t-designs on Hypergraphs, *Discrete Math.* **26** (1985),263-296.

[5] E.S. Kramer, D.W. Leavitt and S.S. Magliveras, Construction procedures for t-designs and the existence of new simple 6-design s, *Ann. Discrete Math.* **26** (1985) 247-274.

[6] D.L. Kreher, An infinite family of (simple) 6-designs, *Journal of Combinatorial Designs* **1** (1993) 277-280.

[7] D.L. Kreher, Simple t-designs with large t: A survey, *JCMCC* **15** (1994), 97-110.

[8] D.L. Kreher and S.P. Radziszowski, The existence of simple 6-(14,7,4) designs, *Journal of Combinatorial Theory (A)* **43** (1986) 237-243.

[9] D.L. Kreher and S.P. Radziszowski, Constructing 6-(14,7,4) Designs, *Contemporary Mathematics,* **111** (1990), 137-151.

[10] A.K. Lenstra, H.W. Lenstra, L. Lovaáz, Factoring Polynomials with Rational Coefficients, *Mathematische Annalen* **261** (1982), 515-534.

[11] S.S. Magliveras and D.W. Leavitt, Simple 6-$(33, 8, 36)$ designs from $P\Gamma L_2(32)$. *Computational Group Theory*, M.D. Atkinson ed., Academic Press 1984, 337-352.

[12] C. P. Schnorr, A More Efficient Algorithm for Lattice Basis Reduction. *J. Algorithms* **9** (1988), 47–62.

[13] C. P. Schnorr and M. Euchner, Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Proceedings of Fundamentals of Computation Theory 91* in *Lecture Notes in Computer Science* **529** (1991), 68–85.

[14] L. Teirlinck, Non-trivial t-designs exist for all t, *Discrete Math.* **65** (1987) 345-356.

[15] L. Teirlinck, Locally trivial t-designs and t-designs without repeated blocks, *Discrete Math.* **77** (1989) 345-356.

[16] B. Schmalz, The t-designs with prescribed automorphism group, new simple 6-designs, *Journal of Combinatorial Designs* **1** (1993), 125-170.