Constructing Combinatorial Designs

Don Kreher

Michigan Technological University

Kreher@mtu.edu

References:

- C.J. Colbourn and J.H. Dinitz (Eds), *The Crc Handbook of Combinatorial Designs* CRC press, LLC (1996).

- D.L. Kreher and D.R. Stinson, *Combinatorial Algorithms: Generation, Enumeration and Search* CRC press, LLC (1998).

A $t-(v,k,\lambda)$ design is a pair$(\mathcal{X},\mathcal{B})$ where:

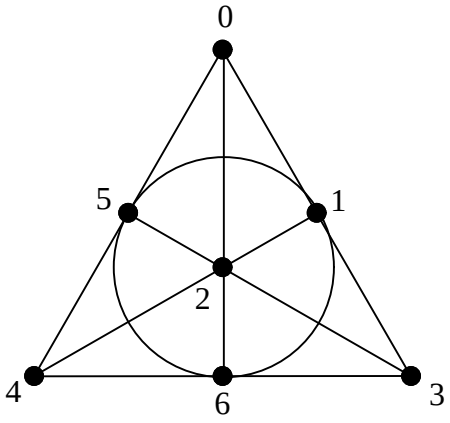
- $\mathcal{X}$ is a v-element set of *points*;
- $\mathcal{B}$ is a family of k-elements subsets of $\mathcal{X}$, called *blocks*;
- every t-element subset $T \subseteq \mathcal{X}$ is contained in exactly λ blocks.

Example:

A 2-(7,3,1) design $(\mathcal{X},\mathcal{B})$ is given by:

$\mathcal{X} = \{0,1,2,3,4,5,6\}$

$\mathcal{B} = \{130, 124, 235, 346, 450, 156, 260\}$



NOTE: $G = \langle\, (0,3,4)(1,6,5)\ ,\ (1,5)(3,4)\,\rangle$

$$= \left\{ \begin{array}{l} \mathrm{I} = (0)(1)(2)(3)(4)(5)(6) \\ (1,3,4)(1,6,5) \\ (1,4,3)(1,5,6) \\ (1,5)(3,4) \\ (1,6)(0,4) \\ (5,6)(0,3) \end{array} \right\}$$

is an obvious automorphism group.

A permutation f on a set X is a one to one function $f : X \mapsto X$.

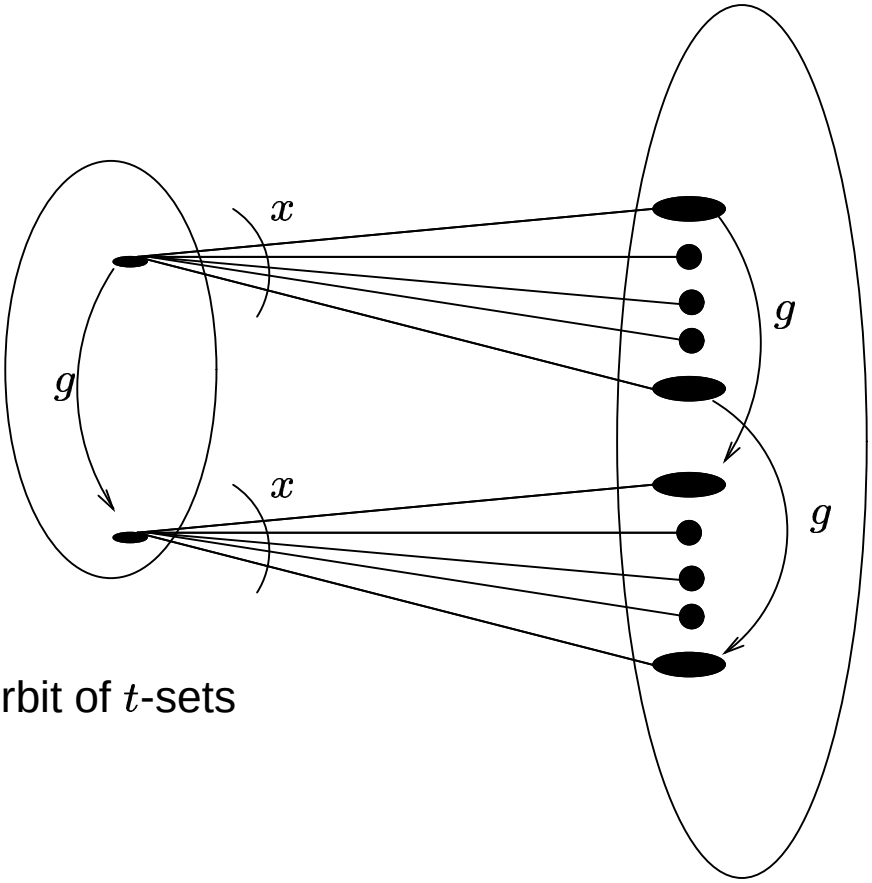
An automorphism of a design $(X, \mathcal{B})$ is a permutation that preserves the blocks.

For example:

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 4 & 0 & 1 & 5 \end{pmatrix} = (0,3,4)(1,6,5)$$

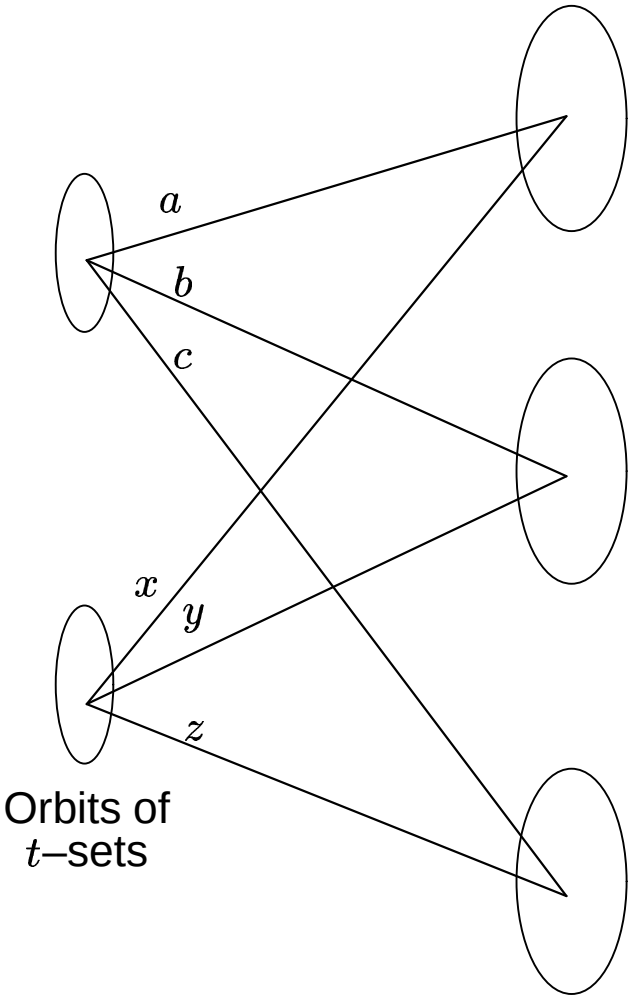
is an automorphism of the 2-(7,3,1) design

$$\begin{array}{cc} 013 & 346 \\ 124 & 024 \\ 235 & 124 \\ 346 \xrightarrow{f} & 045 \\ 045 & 013 \\ 156 & 156 \\ 026 & 235 \end{array}$$



Orbit of t-sets

Orbit of k-sets



$\Rightarrow$

a	b	c
x	y	z

Given integer $0 < t < k < v$, v-set $\mathcal{X}$ and $G \leq Sym(\mathcal{X})$ 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.

Example: $G = \langle (1,4,5)(2,0,6), (2,6)(4,5) \rangle$

	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
{12 40 16 56 50 24}	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
		↑					↑			↑

Kramer and Mesner 1973

A t-(v, k, λ) design exists with $G \leq Sym(\mathcal{X})$ 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: $J = [1, 1, 1, \ldots, 1]^T$.

"The method"

- Choose parameters t, k, v, and λ;
- Find a candidate for an automorphism group G;
- Generate the incidence matrix A_{tk};
- Solve the system of equations $A_{tk}U = \lambda J$ for one, some or all (0,1)-vectors U;
- Check for any special properties you may require of the found solutions;
- Apply any known recursive methods to the solutions found to construct more designs.

Almost every known t-design with $t \geq 6$ was either found this way
or obtained from a design found this way.

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

Find a (0,1)-vector U such that:

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

Such U gives a $t-(v,k,\lambda)$ design with automorphism group G.

Method:

Let $\mathcal{B}$ be the set of columns of $\begin{bmatrix} I & 0 \\ A_{tk} & -\lambda J \end{bmatrix}$.

Let $\mathcal{L} = Span(\mathcal{B}) \subset Z^{n+m}$

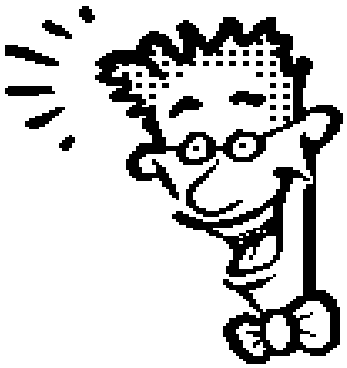
Then: $\mathbf{U} = \begin{bmatrix} U \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ is a short vector of $\mathcal{L}$, $\quad ||\mathbf{U}|| < n$.

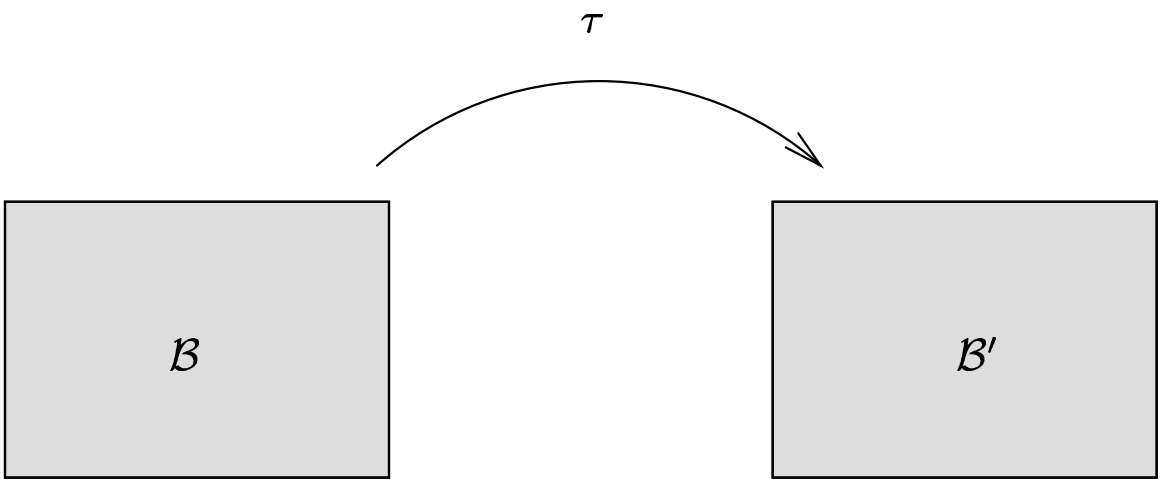
Conversely, if $\begin{bmatrix} U \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathcal{L}$, with U a $(0,1)$–vector,

then $A_{tk}U = m\lambda J$ for some integer m and

a t–$(v, k, m\lambda)$ design is found.

Find transformations $\tau : \mathcal{B} \rightarrow \mathcal{B}'$ so that the vectors in $\mathcal{B}'$ have shorter length.





Tools:

(1) L^3 algorithm, [Lagarias and Odylzko 1982]

Given a basis $\mathcal{B}$ of lattice $\mathcal{L} \in Z^r$ 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 (integer approx. to Gram-Schmidt orthogonalization).

iii. $\mathcal{B}'$ contains short vectors.

proved:
Shorter than $2^n \cdot$(length of shortest nonzero vector in $\mathcal{L}$.

practice:
Much much better!!!

(2) Improvements by Kreher and Radziszowski 1986.

(3) Improvements by Schnor and Euchner 1988/1991.

The $\mathbf{L}^3$ Algorithm
A reduced basis algorithm

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

Step 0 Let $\mathcal{B} = [b_1, b_2, \ldots, b_n]$ be a basis for lattice $\mathcal{L}$.

Step 1 Let $\mathcal{B}^* = [b_1^*, b_2^*, \ldots, b_n^*]$ be the GRAM–SCHMIDT orthogonalization of $\mathcal{B}$.

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

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

Step 2 For $j = 2$ to n

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

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

Step 3 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.

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.

Step 0

$$\text{Set } \mathcal{B} = \begin{bmatrix} I & \vec{0} \\ A & -R \end{bmatrix}, \text{ and } \bar{\mathcal{B}} = \begin{bmatrix} I & \vec{0} \\ A & AJ - R \end{bmatrix},$$

Step 1 Consider the lattice $\mathcal{L}(\mathcal{B})$ where $\mathcal{B}$ is the matrix given above.

Step 2 Find a reduced basis $\mathcal{B}'$ of $\mathcal{L}(\mathcal{B})$.

Step 3 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 $AU = R$.

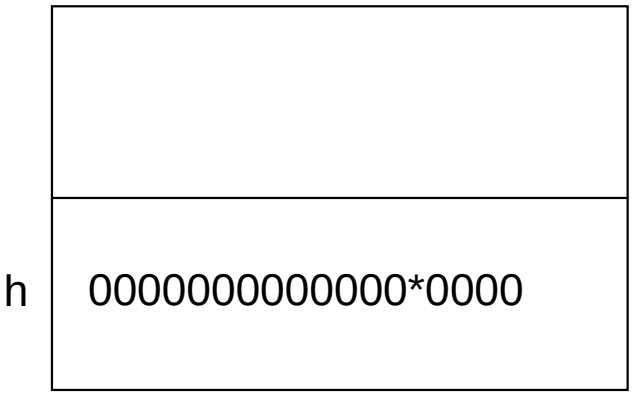
Step 4 Repeat Steps 1 to 3 with $\mathcal{B}$ replaced with $\bar{\mathcal{B}}$. If a vector $[\pm U, \vec{0}]$ with $U \in \{0, 1\}^n$. is found as column of the new reduced basis, then $J - U$ solves $AU = R$. Otherwise, stop. No solution has been found.

Size-Reduction

$$\mathcal{B} = \begin{bmatrix} I & \vec{0} \\ A & -R \end{bmatrix} \begin{matrix} \longrightarrow 1's \text{ and } 0's \\ \longrightarrow 0's \end{matrix}$$

Multiply row h by $c = \max_i ||b_i||^2$

L^3



Delete row h and column j

j

Weight-Reduction

Find $\vec{b_1}, \vec{b_2}, \ldots, \vec{b_k} \in \mathcal{B}$ so that

(1) $||\vec{b_1}|| \leq ||\vec{b_2}|| \leq \ldots ||\vec{b_k}||$ and

(2) $\vec{v} = \epsilon_1 \vec{b_1} + \epsilon_2 \vec{b_2} + \cdots + \epsilon_k \vec{b_k}$ has length $||\vec{v}|| < ||\vec{b_k}||$

Replace $\vec{b_k}$ by $\vec{v}$.

Use $\epsilon_i \in \{+1, -1\}$

A necessary condition is $\sum_{j=1}^{k-1} ||\vec{b_i}||^2 < \sum_{i \neq j} |\vec{b_i} \cdot \vec{b_j}|$.

Consider the complete graph on $\mathcal{B}$

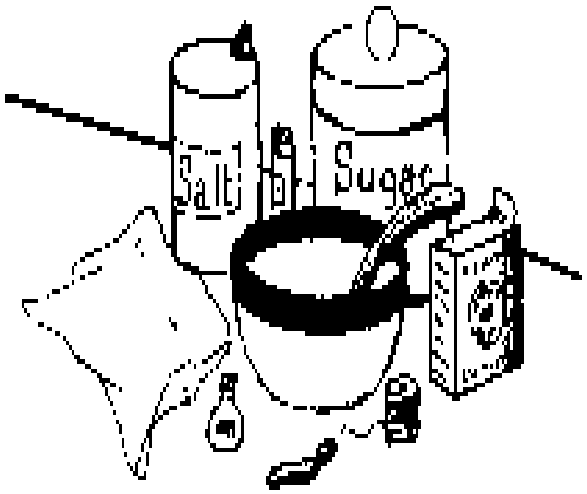
Label the edge $\{\vec{b_i}, \vec{b_j}\}$ by $|\vec{b_i} \cdot \vec{b_j}|$

Keep only those edges that exceed some threshold

Search for k-cliques — they give good candidates.

Basis reduction algorithm
of Kreher and Radziszowski

Input basis $\mathcal{B}$;
$\mathcal{B} := \mathrm{L}^3(\mathcal{B})$;
$\mathcal{B}$:=Size-Reduction($\mathcal{B}$);
currentWeight := $\sum_{\vec{b}\in\mathcal{B}} ||\vec{b}||^2$;
repeat
oldWeight := *currentWeight*;
$\mathcal{B} := \mathrm{Weight\text{-}Reduction}(\mathcal{B})$;
Sort the vectors in $\mathcal{B}$ into order of non-decreasing $||\cdot||$;
$\mathcal{B} := \mathrm{L}^3(\mathcal{B})$;
currentWeight := $\sum_{\vec{b}\in\mathcal{B}} ||\vec{b}||^2$;
until *currentWeight = oldWeight* **or** *solution found*;



Available ingredients

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

$t-(v,t+1,1)$ designs

$t=1$: exist if and only if $v \equiv 0 (\mathrm{mod} 2)$.

$t=2$: exist if and only if $v \equiv 1$ or $3 (\mathrm{mod} 6)$. (Kirkman 1847)

$t=3$: exist if and only if $v \equiv 2$ or $4 (\mathrm{mod} 6)$. (Hanani 1960)

$t=4$: Only ones known have:
$v=11$ (Carmichael 1937, Witt 1938);
$v=23, 47$ and 83 (Denniston 1976);
$v=71$ (Mills 1978) ;
$v=107$ (Grannell and Griggs 1991). $v=131$ (Mathon 1991)

Smallest unsettled parameter set is 4-(17,5,1).

$t=5$: Only ones known have:
$v=12$ (Carmichael 1937, Witt 1938);
$v=24, 48$ and 84 (Denniston 1976);
$v=72$ (Mills 1978);
$v=108$ (Grannell and Griggs 1991). $v=132$ (Mathon 1991)

Smallest unsettled parameter set is 5-(18,6,1).

$t \geq 6$: None are known.

Smallest unsettled parameter set is 6-(19,7,1).

$t-(v,k,1)$ designs, $k \neq t+1$.

$t=1$: exist if and only if $v \equiv 0 (\mathrm{mod} k)$.

$t=2$: For all k there is a v_0 such that for all $v > v_0$ there exists a $2-(v,k,1)$ whenever $v(v-1) \equiv 0 (\mathrm{mod} k)$ and $(v-1) \equiv 0 (\mathrm{mod}(k-1))$ (Wilson 1975).

Smallest unsettled parameter set is 2-(46,6,1).

$t=3$: Only ones known have:
$(v,k) = (q^n+1, q+1)$, $n \geq 2$, q a prime power;
$(v,k) = (22,6)$ (Carmichael 1937, Witt 1938);
$(v,k) = (25,5)$ (Denniston 1976)

Smallest unsettled parameter set is 3-(42,6,1).

$t=4$: Only ones known have:
$(v,k) = (23,7)$ (Carmichael 1937, Witt 1938);
$(v,k) = (27,6)$ (Denniston 1976)

Smallest unsettled parameter set is 4-(42,6,1).

$t=5$: Only ones known have:
$(v,k) = (24,8)$ (Carmichael 1937, Witt 1938);
$(v,k) = (28,7)$ (Denniston 1976)

Smallest unsettled parameter set is 5-(43,7,1).

$t \geq 6$: None are known.

Smallest unsettled parameter set is 6-(29,8,1).

$t-(v,t+1,\lambda)$ designs, $\lambda \neq 1$.

$t=1$: exist if and only if $v\lambda \equiv 0(\mathrm{mod}2)$.

$t=2$: exist if and only if $v(v-1)\lambda \equiv 0(\mathrm{mod}3)$ and $(v-1)\lambda \equiv (0\mathrm{mod}2)$
(Hanani 1961, 1975).

$t=3$: The necessary conditions are know to be sufficient when:
$\lambda = 2$ (Hartman and Phelps);
$\lambda \equiv 0(\mathrm{mod}3)$ and $\lambda < v-3$ (Teirlinck 1984);
for all λ when $v = 5 \cdot 2^n$ (Etzion, Hartman 1990).
Other sporadic results are also known.
Smallest unknown is 3-(25,4,4).

$t=4$: The only known infinite families are:
$4-(4+8u,5,4u)$ for all $u>0$
(Teirlinck 1989, plus Kreher and Radziszowski 1986)
$4-(v,5,\lambda)$ for all $v \equiv 4(\mathrm{mod}\lambda)$ where $\lambda = 2641807540224$ (Teirlinck 1987)
Sporadic examples are also known.
Smallest unknown is 4-(15,5,2).

$t=5$: The only known infinite families known are:
$5-(5+8u,6,4u)$ for all $u>0$
(Teirlinck 1989, plus Kreher and Radziszowski 1986)
$5-(v,6,\lambda)$ for all $v \equiv 5(\mathrm{mod}\lambda)$ where $\lambda = 743008370688000000000000$
(Teirlinck 1987)
Sporadic examples are also known.
Smallest unknown is 5-(16,6,2).

$t = 6$: The only known infinite families are:
$6 - (6 + 8u, 7, 4u)$ for all $u > 0$
(Teirlinck 1989, plus Kreher and Radziszowski 1986)
$6 - (v, 7, \lambda)$ $\forall v \equiv 6 (\mathrm{mod} \lambda)$,
$\lambda = 139740551724710468203315200000000000000$
(Teirlinck 1987)
Seven other examples are known. (Betten et al. 1995)
Smallest unknown is 6-(15,7,3).

$t \geq 7$: The only known infinite family is:
$t - (v, t + 1, \lambda)$ for all $v \equiv t (\mathrm{mod} \lambda)$ where $\lambda = (t + 1)!^{2t+1}$ (Teirlinck 1987)
Seven other examples are known. (Betten et al. 1995)
No other $t - (v, t + 1, \lambda)$ designs are known.
Smallest unknown is 7-(16,8,3).

$t-(v,k,\lambda)$ designs, $\lambda \neq 1$, $k \neq t+1$.

$t=1$: exist if and only if $v\lambda \equiv 0 (\mathrm{mod} k)$.

$t=2$: For all k, λ there is a v_0 such that for all $v > v_0$ there exists a $2-(v,k,\lambda)$ whenever $\lambda v(v-1) \equiv 0 (\mathrm{mod} k)$ and $\lambda(v-1) \equiv 0 (\mathrm{mod}(k-1))$
(Wilson 1975).

Smallest unsettled parameter set is 2-(22,8,4).

$t=3$: Several infinite families and many sporadic examples are known.

Smallest unsettled parameter set is 3-(16,7,5).

$t=4$: There are **TWELVE** or so infinite families known,
(Alltop 1972, Bierbrauer 1989, Hubaut 1974, Driessen 1978 Magliveras and Plambeck 1987, Van Trung 1984 & 1986);
Many sporadic examples.

Smallest unsettled parameter set is 4-(12,6,6).

$t=5$: There are **SIX** infinite families known.,
(Alltop 1972, Magliveras and Plambeck 1987, Van Trung 1984 & 1986);
Many sporadic examples are known.

Smallest unsettled parameter set is 5-(13,7,6).

$t=6$: The only known infinite family is: $6-(23+16m, 8, 4(m+1)(16m+17)$ for $m \geq 0$, (Kreher 1992).
thirty five other examples are known.
Smallest unsettled parameter set is 6-(16,8,15).

$t = 7$: No infinite family is known.
Ten examples are known.
Smallest unsettled parameter set is 7-(18,9,5).

$t \geq 8$: None are known.
Smallest unsettled parameter set is 8-(20,10,6).