Resolvable t-Designs

Reinhard Laue

Reinhard Laue
Department of Mathematics, University of Bayreuth,
95440 Bayreuth, Germany
`laue@uni-bayreuth.de`

Keywords t-design, resolvable, group action, visualization

Abstract

A general group theoretic approach is used to find resolvable designs. Infinitely many resolvable 3-designs are obtained where each is block transitive under some $PSL(2,p^f)$ or $PGL(2,p^f)$. Some known Steiner 5-designs are assembled from such resolvable 3-designs such that they are also resolvable. We give some visualizations of Steiner systems which make resolvability obvious.

1 Introduction

A t-(v,k,λ) design $\mathcal{D}=(V,\mathcal{B})$ is defined on a set V of size v and consists of a family $\mathcal{B}$ of k-element subsets of V approximating all k-element subsets of V such that each t-element subset of V is contained in exactly λ members of $\mathcal{B}$. The k-element subsets in $\mathcal{B}$ are called blocks. If no k-element subset appears twice as a block the t-design is simple. In this article we only consider simple t-designs. A partition of V into k-element subsets is called a spread. Thus, a spread is a 1-$(v,k,1)$ design. Blocks forming a spread form a parallel class resembling lines in geometry that are parallel if they don't intersect. A partition of $\mathcal{B}$ into parallel classes is a resolution. A t-design that admits a resolution is resolvable.

If a t-(v,k,λ) design is resolvable then k divides v. It is not clear when this condition is sufficient. Even then there may be different values of λ possible. Lastly, for the same parameters there may be different isomorphism types of resolvable designs. Thus, there are many open questions.

Resolutions of t-designs have been studied mostly for 2-designs. A recent classification of all resolvable 2-$(14,7,12)$ and 3-$(14,7,5)$ designs is by P. Kaski, L. B. Morales, P. R. J. Östergard, D. A. Rosenblueth, and C. Velarde [6]. Some results for higher values of t have been obtained by Tran van Trung [12], [13], [8], and Liebler, Magliveras, and Tsaranov [10]. The latter authors use a different definition of resolvability that asks for decompositions into smaller designs which need not be spreads but on the other hand decomposes the trivial design that consists of all k-sets. We use a basic tool from [10] to obtain designs that are resolvable in the sense of the standard definition. This will allow to construct resolvable t-(v, k, λ) designs for many divisors k of v when $v = p^f + 1$ for some prime p.

While the automorphism groups of the resolvable designs classified in [6] have an order of at most 156, different infinite families of resolvable block-transitive 3-designs admit the large automorphism groups $PGL(2, q)$ and, in the case of $q \equiv 3 \ mod \ 4$, also $PSL(2, q)$. They are obtained using Dickson's analysis of the subgroups of $PSL(2, q)$ [4, 5] and some group theoretic arguments. The idea is to first prescribe a stabilizer U of a block B and then an overgroup H of U which maps B onto disjoint copies, thereby partitioning the whole projective line.

Corresponding to the different types of subgroups chosen for H we denote the designs to be of *dihedral*, *projective*, *tetrahedral*, *cubical*, or *icosahedral* type. There may result the same parameters for different constructions. The different types are of interest for assembling resolvable t-designs from these 3-designs for $t > 3$, since then the entries of the Kramer Mesner matrix in the columns of these orbits may differ.

The results are summarized in Table 1. Each row describes an infinite series of block-transitive resolvable 3-(v, k, λ) designs. In each case $v = p^f + 1$ for some prime power p^f. The notion $t|f$ here means that t is a proper non-trivial divisor of f. We abbreviate $PSL(2, q)$ by $S(q)$ and $PGL(2, q)$ by $G(q)$ in Table 1.

It should be remarked that the cases where $U = C_2$ or $U = \{id\}$ are not covered. We only give examples in section 8.

In all but one series these designs can be visualized in the following way. The orbits of H on the projective line are determined. For each orbit a solid Γ is needed such that the permutation representation of H on the orbit is the automorphism group of Γ. For a visualization of the solids by a 3-dimensional placement we use our WEB-database of graphs [7]. The projective line has to be identified with the vertices of these solids. A block consists of a set B of k vertices which is invariant under the subgroup U. Thus, a block can be visualized by giving the vertices of the block a peculiar color. This determines a pattern on the set of solids such that its orbit under H is a partition of the point set, visualizing a spread formed by blocks. The parallel classes of spreads are obtained by renaming the vertices according to representatives from the cosets of H in the full group. Each of these will lead to the same drawing with only different names of the vertices.

Some of the known Steiner 5-systems are composed from such resolvable 3-designs. In particular, one of Denniston's Steiner 5-designs on 24 points is shown to be resolvable. We also visualize further resolvable 3-designs

Table 1: Resolvable 3-(v,k,λ) Designs

Group	v	k	λ	*Condition*	U	H
$G(q)$	$q+1$	$\frac{q+1}{2}$	6	$q>5$	$D_{\frac{q+1}{2}}$	D_{q+1}
$G(q)$	$q+1$	$5<k$ $k\mid\frac{q+1}{2}$	$(k-1)(k-2)/2$	$\gcd(k,p^t+1)=$ 1 if $t\mid f$, $t<f$	D_k	$D_{\frac{q+1}{2}}$
$G(q)$	$4x$	$k=5$ $k\mid\frac{q+1}{2}$	$(k-1)(k-2)/2$	$\gcd(k,p^t+1)=$ 1 if $t\mid f$, $t<f$	D_k	$D_{\frac{q+1}{2}}$
$S(q^f)$	f odd $4x$	$\frac{q^f-q}{q+1}+1$	$((\frac{q^f-q}{q+1})^2-1)\frac{q^{f-1}-1}{q^2-1}$	$\gcd(k,q^t+1)=$ 1 if $t\mid f$, $t<f$	H_α	$S(q)$
$S(3^f)$	f odd $12x+4$	$3x+1$	$(3x+1)x(3x-1)/2$	$\gcd(k,3^t+1)=$ 1 if $t\mid f$, $t<f$	C_3	A_4
$S(p^f)$	12x + 8	$3x+2$	$(3x+2)(3x+1)x/2$	$\gcd(k,p^t+1)=$ 1 if $t\mid f$, $t<f$	C_3	A_4
$S(q)$	$24x$	$6x$	$x(6x-1)(3x-1)$		D_3	S_4
$S(q)$	$24x$	$8x$	$x(8x-1)(4x-1)$		D_4	S_4
$S(q)$	$60x$	$12x$	$x(12x-1)(6x-1)$		A_4	A_5
$S(q)$	$60x$	$10x$	$x(10x-1)(5x-1)$		D_5	A_5
$S(q)$	$60x$	$5x$	$x(5(x-1)/2+2)(5x-2)$	x *odd*	C_5	A_5
$S(q)$	$60x+12$	$5x+1$	$(5x+1)x(5x-1)/2$		C_5	A_5
$S(q)$	$60x+12$	$10x+2$	$(5x+1)(10x+1)x$		D_5	A_5
$S(q)$	$60x+20$	$3x+1$	$x(3x+1)(3x-1)/2$		C_3	A_5
$S(q)$	$60x+20$	$6x+2$	$x(3x+1)(6x+1)$		D_3	A_5
$G(q)$	$60x+30$	$6x+3$	$(2x+1)(3x+1)(6x+1)$		D_3	A_5
$G(q)$	$60x+30$	$10x+5$	$(2x+1)(5x+2)(10x+3)$		D_5	A_5
$G(q)$	$60x+30$	$12x+6$	$(2x+1)(12x+5)(6x+2)$		A_4	A_5
$G(q)$	$60x+42$	$10x+7$	$(10x+7)(5x+3)(2x+1)$		D_5	A_5
$G(q)$	$60x+50$	$6x+5$	$(6x+5)(3x+2)(2x+1)$		D_3	A_5

and resolvable Steiner systems with the parameters 3-$(8,4,1)$, 5-$(12,6,1)$, 5-$(24,6,1)$, 5-$(24,8,1)$.

2 Basic Tools

A group G of permutations on a set V is prescribed as a group of automorphisms of t-(v,k,λ) designs. These t-designs are obtained as collections of orbits of G on all k-element subsets of V. We select orbits such that each of them is already a resolvable s-design for some $s\le t$. The selection of orbits is done by first prescribing a stabilizer U of k-element subsets and an overgroup H of U. Among the k-element subsets with stabilizer U those are chosen whose orbit under H form a partition of V. This strategy is made precise and justified by the following Lemmata.

A decomposition of an orbit on k-element subsets of V into disjoint classes can be obtained by a classical group theoretic result.

Lemma 2.1 *Let a group G act transitively on a set Ω such that the stabilizer $U = G_\omega$ of some $\omega \in \Omega$ is contained in some subgroup H of G. Then $\omega^H = \{\omega^h | h \in H\}$ is a set of imprimitivity.*

In our context, Ω is an orbit of G on k-element subsets of V and ω a representative B that will become a block of a design. A crucial point in the construction is to select B such that all B^h for $h \in H$ in Lemma 2.1 form a spread. We use the following generalization of Proposition 2.1 in [10].

Lemma 2.2 *Let a group G act on a set V, and let $U < H < G$ where U is the set-stabilizer of a subset B of V such that $\frac{|H|}{|U|} = \frac{|V|}{|B|}$. For each orbit V_i of H on V let U be the set-stabilizer in H of the intersection $B_i = V_i \cap B$. Then $B^H = \{B^h | h \in H\}$ is a spread and the orbit B^G decomposes into $|G|/|H|$ parallel classes of spreads. If, in addition, G acts t-homogeneously on V then B^G is a resolvable t-design.*

Proof. By the assumption,

$$\bigcup_{h\in H} B^h = \bigcup_{h\in H}\bigcup_{i} B_i^h = \bigcup_{i}\bigcup_{h\in H} B_i^h = \bigcup_{i} V_i = V.$$

The orbit of B under H consists of $\frac{|H|}{|U|}$ sets B^h of size $|B|$ such that these can cover all points of V only if the sets are disjoint. Therefore they form a spread. By Lemma 2.1 the orbit B^G decomposes into sets of imprimitivity, that form parallel classes. If G is t-homogeneous then each t-element subset is contained in the same number of k-element subsets from the same orbit. So, each orbit on k-sets forms a t-design then. ∎

Several resolvable designs can already be obtained from the special case of a transitive H. A cyclic such H is for example considered in the point cyclic resolutions of [11]. An easy generalization of that is a regular action of H.

For a given subgroup U, if we form a union of some orbits of U on V, we obtain a set B that is invariant under U. Some additional requirements will be needed to assure that U is the full set stabilizer of B in G. In a special case this can be proved easily.

Lemma 2.3 *Let U be a subgroup of a permutation group G such that U acts fixed point freely and has order k. If no non-trivial element of G leaves any $k-1$-element subset invariant then U is the full set-stabilizer in G of each of its orbits.*

Proof. Let S be the full set stabilizer S of a U-orbit B. For any point $x \in B$ the stabilizer S_x of x in B leaves invariant $B \setminus \{x\}$. This is a (k-1)-element subset such that by the assumption $S_x = \{id\}$. So, S acts fixed point freely on B and has order dividing k. Since U is contained in S and U is transitive on B, we have $S = U$. ■

A non-regular action of H is more complicated to analyse. In the case of the groups $PSL(2,q)$ or $PGL(2,q)$ the following general situation occurs frequently.

Lemma 2.4 *Let a group G act on a set V. Let $U < H < G$ and $U < D < G$ and D cyclic or dihedral. In case of a dihedral D let either U be dihedral or U cyclic and 4 no divisor of $|D : U|$ or let $s|U|$ be odd and D fixed point free. Let $W \subseteq V$ such that H acts semiregularly on W with orbits W_i, $i = 1, \cdots, s$. Then there exists a selection of exactly one U-orbit B_i from each W_i such that U is the set-stabilizer of $B = \bigcup_{1 \le i \le s} B_i$ in D.*

Proof. There is some freedom in choosing one of the U-orbits in an H-orbit. We make use of that to find a B such that U is the full set-stabilizer of B in D. Suppose we have chosen the B_i so that U is not the full set-stabilizer of B. Then there is a proper overgroup $A \le D$ stabilizing B. So, B is a union of A-orbits which each decomposes into U-orbits, since U is contained in A. Let $|A : U| = \prod_{1 \le i \le s} p_i^{a_i}$ be the prime power factorization. Then for each odd p_i there exists at most one subgroup A_i such that $|A_i : U| = p_i$. If there exists more than one such subgroup for $p_i = 2$ then 4 divides $|D : U|$ and U is cyclic which is excluded. If $s|U| = |B|$ is odd then an overgroup A of order $2|U|$ would have an element of order two that must have fixed points on a set of odd size, contrary to our assumption that D is fixed point free.

We consider the orbit O_1 of the first U-orbit B_1 under A_1. Because A_1 leaves B invariant O_1 consists of U-orbits, each taken from exactly one H-orbit. We then in one of these H-orbits replace the chosen U-orbit by another U-orbit. Then B is no longer invariant under A_1. We continue with A_2 by considering only the remaining H-orbits in the same way. Since the sum of the r_i is smaller than their product, there are enough H-orbits to continue until no A_i leaves B invariant. ■

The prescribed groups of automorphisms will be $PSL(2,q)$ or $PGL(2,q)$ for $q = p^f$ a power of a prime p. We recall that for $q = p^f \equiv 3 \bmod 4$ the group $PSL(2,q)$ is 3-homogeneous. In our constructions we will heavily make use of Dickson's classification of all subgroups of $PSL(2,q)$, see for example [5]. There exist only

- Dihedral groups of an order dividing $(p^f + 1)$ or $(p^f - 1)$ for odd p, resp. $2(2^f + 1)$ or $2(2^f - 1)$ for $p = 2$, and their cyclic subgroups,

- $PSL(2,p^t)$ if $t|f$ and $PGL(2,p^t)$ if $2t|f$, their point stabilizers as semidirect products of an elementary abelian subgroup of order p^t by cyclic subgroups of an order dividing (p^f-1) and (p^t-1) and their elementary abelian p-subgroups,
- Tetrahedral subgroups isomorphic to A_4,
- Cubical subgroups isomorphic to S_4,
- Icosahedral subgroups isomorphic to A_5.

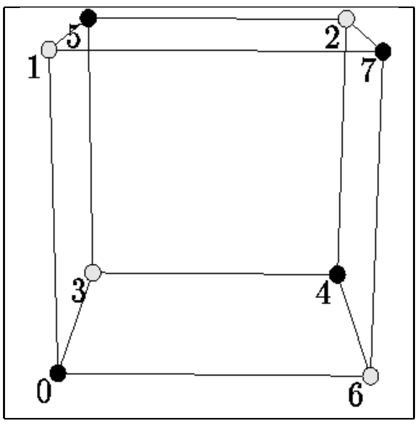
Some divisibility conditions rule out some of these subgroups in some cases. The cubical subgroups are called octahedral subgroups in the classical literature. We prefer the notion cubical subgroup, since the permutations in these groups defined on the projective line act as automorphisms of a cube or a truncated cube for an appropriate labelling of these solids, see Tables 2, 4.

An example for our approach is a construction of the 3-$(8,4,1)$ design. The chain of subgroups of the automorphism group is

$$G = PSL(2,7) > H \cong S_4,\ H > U \cong A_4.$$

The subgroup H can be represented as the automorphism group of a cube whose vertices are the 8 points of the projective line $PG(1,7)$. A permutation representation can be obtained by Theorem 8.1. The subgroup U is the automorphism group of two disjoint tetrahedra which are embedded in the cube. This group is the set stabilizer of the set B of the points that belong to one of the tetrahedra. So, the orbit of B under $PSL(2,7)$ decomposes into $PSL(2,7):H = 7$ parallel classes of 2 blocks. This orbit forms a resolvable 3-$(8,4,1)$ design.

Table 2: A 3-(8,4,1) Design from $PSL(2,7)$



Generally, the stabilizers of 2 points have order $(p^f - 1)/2$. So, if this order is odd then no group element of order 2 in $PSL(2,q)$ may fix any point.

As our groups H we choose the Dihedral groups of an order dividing $(p^f + 1)$, the projective groups $PSL(2,p^t)$ if $t|f$, tetrahedral, cubical, and icosahedral subgroups. The subgroups U are taken within these groups so that they are the full set stabilizers of certain sets assembled from their orbits. The difficult part always will be to show that U is the full set stabilizer. The easiest cases are large subgroups U while orders less or equal to 5 are more and more difficult cases.

The number of blocks b is the index of U in $PGL(2,q)$ or $PSL(2,q)$ such that the parameter λ results from the formula

$$\lambda = b\frac{\binom{k}{t}}{\binom{v}{t}}.$$

For $t = 3$, q odd and $PSL(2,q)$ this evaluates to

$$\lambda = \frac{k(k-1)(k-2)}{2|U|}.$$

We have to determine the types of the orbits of subgroups H of $G = PSL(2,p^t)$. Recall that the type of an orbit is determined by the conjugacy class of the stabilizers. One could use Burnside's Lemma [9]. This would require the knowledge of the action of each subgroup of H. In our cases we only need the number of fixed points of the elements of H like in the Cauchy-Frobenius Lemma. An element $x \in H$ fixes a coset Ug of a stabilizer $U = H_\alpha$ in the right multiplication action if and only if x fixes α^g. The number of fixed points on an orbit of some type can be found by computation within the group by Lemma 2.5.

Lemma 2.5 *Let $A \leq H$ and $x \in H$ for a finite group H. If x is conjugate to exactly r elements of A in H then X fixes exactly $\frac{r\cdot|C_H(x)|}{|A|}$ cosets Ag of A in H.*

Proof. Let x be conjugate to $x_1, \ldots, x_r \in A$. The equivalence

$$Agx = Ag \Longleftrightarrow Agxg^{-1} = A \Longleftrightarrow \exists_i gxg^{-1} = x_i \Longleftrightarrow g \in \bigcup_{i=1}^{r} g_i C_H(x)$$

shows that

$$\bigcup_{Agx=Ag} Ag = \bigcup_{i=1}^{r} g_i C_H(x).$$

Since all cosets of a subgroup have the same size, this implies the claimed formula. ∎

If the numbers of fixed points of the elements in some action are known then these are composed from the corresponding numbers on the orbits. This gives the linear relation in Lemma 2.6.

Lemma 2.6 *Let a group H act on a set Ω. Let $C_1, \cdots, C_m$ be the conjugacy classes of elements of H and $U_1, \cdots, U_n$ be representatives from the conjugacy classes of subgroups of H. Let M be a $m \times n$ matrix where*

$$M_{i,j} = |\{U_j g | U_j g x = U_j g\}|$$

for any $x \in C_i$. If $f = (f_1, \cdots, f_m)$ is the vector of fixed point numbers $f_i = |\{\omega | \omega^g = \omega\}|$ for $g \in C_i$ and $h = (h_1, \cdots, h_n)$ is the vector of multiplicities h_j with which the type H/U_j appears in Ω then the equation

$$Mh^t = f^t$$

holds.

The proof is immediate. By the preceding Lemma 2.5 the entries of M may be computed. Also the numbers of fixed points will be known from the application. So, the unknown multiplicities form a solution vector for a diophantine set of linear equations. In our application each f_i for a non-identity class is at most two. Then it is easy to determine from the matrix equation the vector of multiplicities.

3 Resolvable 3-Designs of Dihedral Type

We start with resolvable designs where H is the normalizer of a Singer cycle in $PGL(2,q)$.

Theorem 3.1 *For each odd prime power $q > 5$ there exists a block transitive resolvable 3-$(q+1, \frac{q+1}{2}, \frac{(q-1)(q-3)}{8})$ design admitting the automorphism group $PGL(2,q)$.*

Proof. Let q be an odd prime power. Then $PGL(2,q)$ is 3-homogeneous. A Singer cycle S of order $q+1$ contains a unique subgroup C of index 2. This C acts fixed point freely and, thus, has two orbits on the projective line and index 4 in the normalizer H of S. Since H acts on the set of orbits of C, the stabilizer U of an orbit B has index 2 in H. The subgroup U is the full set-stabilizer of B and the orbit of B under $PGL(2,q)$ is a 3-design. The overgroup H maps B onto the other orbit of U which is the complement of B. Thus, by Lemma 2.2, we obtain a resolvable 3-$(q+1, \frac{q+1}{2}, \frac{(q-1)(q-3)}{8})$ design. ■

This construction can be generalized to further divisors k of $v = q+1$ if some additional divisibility conditions are fulfilled.

Theorem 3.2 *Let $q = p^f$ be a power of a prime p and k a divisor of $(q+1)/2$ such that $k > 5$ and gcd(k,$p^t + 1$) $= 1$ for all proper non-trivial divisors t of f. Then there exists a resolvable 3-$(q+1, k, \frac{(k-1)(k-2)}{2})$ design admitting the automorphism group $PGL(2,q)$. If $q \equiv 3$ mod 4 then this holds also for $k = 5$.*

Proof. Let H be a dihedral subgroup of order $2(q+1)$ of $PGL(2,q)$. Then the Singer cycle S of order $q+1$ is the unique cyclic subgroup of this order in H containing a unique subgroup C of order k. Because C is normal in H the orbits of C are blocks of imprimitivity under the action of H. Already S permutes them transitively such that the index of a set stabilizer U of a C-orbit B in H is the same as in S. Thus, U is isomorphic to a dihedral group of order $2k$ and the orbit of B under S is a spread.

It remains to be shown that U is the full set stabilizer of B. Let N be the the full set stabilizer of B in $PGL(2,q)$. Then $N \cap PSL(2,q)$ is the full set stabilizer of B in $PSL(2,q)$ and contains C. The possible overgroups of C are obtained from the classification of the subgroups of $PSL(2,q)$.

Because of the assumptions on k the cyclic group C of order k is not contained in any subgroups of the type A_4, S_5, A_5, or $PSL(2,p^t)$ for $1 < t < f$ of $PSL(2,q)$. Therefore $N \cap PSL(2,q)$ is contained in $H \cap PSL(2,q)$ and is isomorphic to a dihedral group or cyclic of order k. In both cases C is characteristic in $N \cap PSL(2,q)$. By the isomorphism theorem

$$N/(N \cap PSL(2,q) \cong N \cdot PSL(2,q)/PSL(2,q) \leq PGL(2,q)/PSL(2,q)$$

has at most order 2. Therefore $N \cap PSL(2,q)$ is normal in N such that also C is normal in N. But then N is contained in $N_{PGL(2,q)}(C) = H$ and $N = U$.

Since $PGL(2,q)$ is 3-homogeneous, we obtain the claimed resolvable 3-design. If $k = 5$ and 5 divides $q+1$ and $q \equiv 3$ mod 4 then U is a dihedral group of order 10. The only proper overgroup of U in $PSL(2,q)$ not in H is isomorphic to A_5 and has no orbit of length 5 in this case, since otherwise some element of order 2 of A_5 would have a fixed point and for $q \equiv 3$ mod 4 all elements of order 2 in $PSL(2,q)$ are fixed point free. As before we obtain the claimed resolvable 3-design. ∎

Further below a 3-design of this type with parameters 3-$(24,6,10)$ will be described explicitely as part of a resolvable Steiner 5-design.

Note that Theorem 3.2 also holds for $p = 2$. For instance, there exist resolvable 3-$(65,13,396)$ and 3-$(129,43,5166)$ designs.

In some cases the $PGL(2,q)$ orbit forming a 3-$(q+1,5,6)$ design splits into two $PSL(2,q)$ orbits forming resolvable 3-$(q+1,5,3)$ designs. This holds for 3-$(10,5,3)$ and 3-$(50,5,3)$ but not for $q \in \{29,89,169\}$. The general pattern is not yet clear to the author.

4 Resolvable 3-Designs of Projective Type

If q^f is a power of an odd prime such that 4 divides q^f+1 then f is odd and $gcd(q^f-1, q+1) = 2$. This is easily shown by induction on n where $f = 2n+1$. Also, then 4 divides $q+1$ because $q \equiv 1 \ mod\ 4$ would lead to $q^f \equiv 1 \mod 4$. So, any element of $PSL(2,q^f)$ of an order dividing $q+1$ in this case has no fixed points on the projective line $PG(1,q^f)$. This makes it easy to describe the orbit types of the subgroups $PSL(2,q)$ in their action on $PG(1,q^f)$.

Theorem 4.1 *Let $q^f \equiv 3 \ mod\ 4$ for some odd $f > 1$ and some prime power $q > 5$ and let $k = q\frac{q^{f-1}-1}{q+1} + 1$. If $gcd(k, q^t+1) = 1$ for all proper non-trivial divisors t of f then $PSL(2,q^f)$ is a block transitive group of automorphisms of a resolvable*
3-$(q^f+1, q\frac{q^{f-1}-1}{q+1}+1, ((q\frac{q^{f-1}-1}{q+1})^2-1)\frac{q^{f-1}-1}{q^2-1})$ design.

Proof. We employ the group $G = PSL(2,q^f)$ in its natural action on the projective line $L = PG(1,q^f)$. Then $H = PSL(2,q)$ is a subgroup of G containing a subgroup U of order $q\frac{q-1}{2}$. The projective line $L_1 = PG(1,q)$ is contained in L. The subgroup H acts transitively on L_1 in the natural way. U has one fixed point and one orbit of length q on L_1. By the preceding discussion, any element of H different from the identity has the same number of fixed points on L as on L_1. Therefore, no fixed points of such an element lie in $L \setminus L_1$. The subgroup H therefore acts semiregularly on $L \setminus L_1$. We assemble a subset B of L by taking the fixed point of U and an orbit of U of length $q\frac{q-1}{2}$ out of each orbit of H on $L \setminus L_1$. Since H is acting regularly on each orbit O, such an O decomposes into $q+1$ sets of size $q\frac{q-1}{2}$ corresponding to the cosets of U in H.

The result will follow from Lemma 2.2 if U is the full set-stabilizer in G of the set B. So, all proper overgroups of U have to be ruled out as a set-stabilizer of B. For $q > 5$ none of the subgroups isomorphic to A_4, S_4, A_5 and also none of the dihedral groups may contain U. By the divisibility condition also no proper subgroup of the type $PSL(2,q^t)$ may contain U. So, the only possible proper overgroups of U in G are H, a semidirect product of a Sylow subgroup P of G with a subgroup of order $\frac{q-1}{2}$ of U, and the full stabilizer S of a point in G. Since H is contained in S and H does not stabilize B, we are only left with the extension of the Sylow subgroup P. P has one fixed point and acts regularly on the q^f remaining points and therefore cannot stabilize B. Since $G = PSL(2,q^f)$ is 3-homogeneous on L, the orbit B^G is a 3-design.

The block size $k = |B|$ is obtained as $k = 1 + q\frac{q-1}{2} \cdot m$, where m is the number of orbits of H on $L \setminus L_1$, that is

$$m = \frac{(q^f+1)-(q+1)}{(q+1)q(q-1)/2} = 2\frac{q^{f-1}-1}{q^2-1}.$$

Inserting m and cancelling yields $k = 1+q\frac{q^{f-1}-1}{q+1}$. The value of λ is obtained from the general formula. ■

The divisibility conditions are obviously fulfilled if f is a prime so that the theorem applies in infinitely many cases. Some parameter sets obtained are 3-(28,7,35), 3-(344,43,1763), 3-(1332,111,12099), 3-(6860,343,116963).

5 Resolvable 3-Designs of Tetrahedral Type

Theorem 5.1 *Let $p^f + 1 = 12x + 4$. Then $p = 3$ and f is odd. Let $k = 1+\frac{3^f-3}{4}$ and gcd(k,3^t+1) $= 1$ for all proper non-trivial divisors t of f. Then there exists a resolvable 3-$(3^f+1, k, \lambda)$ design, where $\lambda = 1/6\cdot k(k-1)(k-2)$, admitting $PSL(2, 3^f)$ as a block transitive group of automorphisms.*

Let $p^f + 1 = 12x + 8$. If gcd($3x + 2$,$p^t + 1$) $= 1$ for all proper non-trivial divisors t of f then there exists a resolvable 3-$(12x+8, 3x+2, \frac{(3x+2)(3x+1)x}{2})$ design, admitting $PSL(2, p^f)$ as a block transitive group of automorphisms.

Proof. We determine the orbit types of $H \cong A_4$ on the projective line by Lemma 2.6. Consider the matrix M in this case.

Element	Id	C_2	A_3	V_4	A_4
id	12	6	4	3	1
$(1,2)(3,4)$	0	2	3	0	1
$(1,2,3)$	0	0	0	1	1
$(1,3,2)$	0	0	0	1	1

The vector of fixed points on the projective line in the listed cases is given by the following table.

$f(id)$	$12x+4$	$12x+8$
$f((1,2)(3,4))$	0	0
$f((1,2,3))$	1	2
$f((1,3,2))$	1	2

The solution vectors h for the equation $Mh^t = f^t$ are as follows:

Case	$h(Id)$	$h(C_2)$	$h(A_3)$	$h(V_4)$	$h(A_4)$
$12x+4$	x	0	0	1	0
$12x+8$	x	0	0	2	0

This means that H has x regular orbits and 1 or 2 orbits of size 4 on the projective line.

It is clear that $p^f \equiv 3 \bmod 12$ implies that 3 divides p^f. Then 4 divides $3^{f-1}-1$ which is congruent to $(-1)^{f-1}-1 \bmod 4$. Therefore, $f-1$ must be even. Let U be a point stabilizer of order 3 in H. Then U leaves invariant a set B that is composed of the fixed point of U and one U-orbit of size 3 from each H-orbit of size 12. Then this B has $k = 1 + 3 \cdot \frac{3^f-3}{12}$ elements. It remains to be shown that U is the full set stabilizer of B in $PSL(2, 3^f)$. The only possible overgroups are contained in the same Sylow 3-subgroup P as U which is abelian. If an element $g \in P$ of order 3 leaves B invariant then g has to permute the orbits of U that are contained in B because g leaves U invariant. From $3^f \equiv 3 \bmod 12$ we see that B contains $\frac{3^f-3}{12}$ orbits of size 3 of U and this number is not divisible by 3 for $f > 2$. So, g must leave some orbit of U of size 3 invariant. Since P acts regular on the points different from the fixed point, this implies that $g \in U$. The result now follows from Lemma 2.2.

Let $p^f + 1 \equiv 8 \bmod 12$. We choose U as a subgroup of order 3 of $H \cong A_4$ having two fixed points and all other orbits of size 3. We assemble B by taking the fixed points of U from the two H-orbits of size 4 and one U-orbit of size 3 out of each other H-orbit. There result $k = 2 + 3x$ elements for B and $\lambda = (3x + 2)(3x + 1)x/2$. Of course, U is the set stabilizer of B in H. But U is also contained in a dihedral group D of order $p^f - 1$. Because $(p^f - 1)/2$ is odd 4 is no divisor of $|D : U|$. So, by Lemma 2.4 we can choose B such that U is also the set stabilizer of B in D. The result now follows from Lemma 2.2.

■

Theorem 5.1 proves again the existence of a resolvable 3-$(28, 7, 35)$ design.

6 Resolvable 3-Designs of Cubical Type

Theorem 6.1 *Let $p^f + 1 \equiv 0$ mod 24. Then there exists a resolvable 3-$(p^f + 1, k, \lambda)$ design, where $k = \frac{p^f+1}{3}$ and $\lambda = k(k-1)(k-2)/16$ admitting $PSL(2, p^f)$ as a block transitive group of automorphisms. There exists also a resolvable 3-(p^f+1, k, λ) design, where $k = \frac{p^f+1}{4}$ and $\lambda = k(k-1)(k-2)/12$, admitting $PSL(2, p^f)$ as a block transitive group of automorphisms.*

Proof. In this case $PSL(2, p^f)$ contains a subgroup $H \cong S_4$ with a Sylow 2-subgroup $U \cong D_4$. Neither 2 nor 3 divides $p^f \frac{(p^f-1)}{2}$ such that the non-trivial elements of H have no fixed points. Thus, H is semiregular. We can choose from each H-orbit one U-orbit to obtain a block B of size $\frac{p^f+1}{3}$ such that its orbit under H is a partition of the projective line.

If there is a proper overgroup A stabilizing B then A must be contained in the dihedral subgroup of order $(p^f + 1)$ and as such acts semiregular. So, by Lemma 2.4 we can choose B in a way such that U is the full set-stabilizer of B. Now, Lemma 2.2 yields the claimed design.

H also contains a subgroup $U \cong D_3$. The construction and the existence proof with this pair of subgroups are analogous to the preceding case. ■

In section 8 we will discuss the special case $p^f = 23$ in detail.

7 Resolvable 3-Designs of Icosahedral Type

Theorem 7.1 *a) Let $q+1 = 60x$ for some prime power q. Then $PSL(2,q)$ is a block transitive group of automorphisms of resolvable*

3-$(q+1, 12x, x(12x-1)(6x-1))$ *and* 3-$(q+1, 10x, x(10x-1)(5x-1))$ *designs. If x is odd then $PSL(2,q)$ is a block transitive group of automorphisms of resolvable there exists a resolvable*

3-$(q+1, 5x, x(5(x-1)/2+2)(5x-2))$ *design.*

b) Let $q+1 = 60x+12$ for some prime power q. Then $PSL(2,q)$ is a block transitive group of automorphisms of resolvable

3-$(q+1, 5x+1, (5x+1)x(5x-1)/2)$ *and* 3-$(q+1, 10x+2, (5x+1)(10x+1)x)$ *designs.*

c) Let $q+1 = 60x+20$ for some prime power q. Then $PSL(2,q)$ is a block transitive group of automorphisms of resolvable

3-$(q+1, 3x+1, x(3x+1)(3x-1)/2)$ *and* 3-$(q+1, 6x+2, x(3x+1)(6x+1))$ *designs.*

d) Let $q+1 = 60x+30$ for some prime power q. Then $PGL(2,q)$ is a block transitive group of automorphisms of resolvable

3-$(q+1, 6x+3, (2x+1)(3x+1)(6x+1))$, 3-$(q+1, 10x+5, (2x+1)(5x+2)(10x+3))$, *and* 3-$(q+1, 12x+6, (2x+1)(12x+5)(6x+2))$ *designs.*

e) Let $q+1 = 60x+42$ for some prime power q. Then $PGL(2,q)$ is a block transitive group of automorphisms of a resolvable

3-$(q+1, 10x+7, (10x+7)(5x+3)(2x+1))$ *design.*

f) Let $q+1 = 60x+50$ for some prime power q. Then $PGL(2,q)$ is a block transitive group of automorphisms of a resolvable

3-$(q+1, 6x+5, (6x+5)(3x+2)(2x+1))$ *design.*

Proof. Let $q > 5$ be a prime power with q^2-1 divisible by 5. Then a subgroup $H \cong A_5$ is contained in $PSL(2,q)$. We determine the orbit types of H on the projective line by Lemma 2.6. Consider the matrix M in this case.

Element	Id	C_2	C_3	C_5	V_4	S_3	D_5	A_4	A_5
id	60	30	20	12	15	10	6	5	1
$(1,2)(3,4)$	0	2	0	0	3	2	2	1	1
$(1,2,3)$	0	0	2	0	0	1	0	2	1
$(1,2,3,4,5)$	0	0	0	2	0	0	1	0	1
$(1,2,3,5,4)$	0	0	0	2	0	0	1	0	1

The vector of fixed points in the listed cases is given by the following table.

$f(id)$	$60x$	$60x+12$	$60x+20$	$60x+30$	$60x+42$	$60x+50$
$f((1,2)(3,4))$	0	0	0	2	2	2
$f((1,2,3))$	0	0	2	0	0	2
$f((1,2,3,4,5))$	0	2	0	0	2	0
$f((1,2,3,5,4))$	0	2	0	0	2	0

The solution vectors h for the equation $Mh^t = f^t$ are as follows:

$Case$	$h(Id)$	$h(C_2)$	$h(C_3)$	$h(C_5)$
$60x$	x	0	0	0
$60x+12$	x	0	0	1
$60x+20$	x	0	1	0
$60x+30$	x	1	0	0
$60x+42$	x	1	0	1
$60x+50$	x	1	1	0

and $h(V_4) = h(S_3) = h(D_5) = h(A_4) = h(A_5) = 0$ in all cases.

a) In this case, all orbits of H are regular. We choose as U a subgroup of index 5 in H. Then U has orbits of length 12 on each H-orbit. If we choose one U-orbit out of each H-orbit we obtain a set of size $\frac{q+1}{5}$. Since $U \cong A_4$, it is not contained in any dihedral group. It could be contained in a unique overgroup $A \cong S_4$. If this A leaves B invariant we can change our choice of U-orbits such that A no longer leaves B invariant by Lemma 2.4. The claimed parameters follow from the general strategy.

We can also choose U a subgroup of index 6 in H. Then U is dihedral of order 10 and using Lemmata 4 and 2 we obtain a resolvable 3-$(q+1, 10x, x(10x-1)(5x-1))$ design. If x is odd then we can choose U a subgroup of index 12 in H. In this case U is cyclic of order 5 and a choice of one U-orbit from each H-orbit results in a set B of size $5x$. By Lemma 2.4 and Lemma 2.2 we obtain the claimed designs.

b) In this case, H has one orbit of length 12 and the other orbits are regular. We choose as U a subgroup of index 12 in H. Then U has two fixed points and orbits of length 5 on each H-orbit. If we choose one fixed point and one U-orbit out of each H-orbit we obtain a set B of size $5x+1$. Then

$$\lambda = \frac{(5x+1)5x(5x-1)}{2 \cdot 5} = \frac{(5x+1)x(5x-1)}{2}.$$

If we choose as U a subgroup of index 6 in H then B is assembled from the two fixed points of U and an orbit of length 10 from each other H-orbit. Then $k = 10x+2$ and $\lambda = \frac{(10x+2)(10x+1)10x}{2 \cdot 10} = (5x+1)(10x+1)x$.

We apply Lemma 2.4 with W the union of the regular orbits of H. Then in each case B can be chosen such that U is the full set-stabilizer of B. By Lemma 2.2 we obtain the claimed designs.

c) In this case, H has one orbit of length 20 and the other orbits are regular. We choose as U a subgroup of index 20 in H. Then U has orbits of length 3 on each regular H-orbit. We assemble B from a fixed point of U out of the H-orbit of length 20 and one U-orbit out of each regular H-orbit according to Lemma 2.4. Then $|K| = 3x + 1$ and $\lambda = \frac{(3x+1)3x(3x-1)}{2\cdot 3} = \frac{(3x+1)x(3x-1)}{2}$. By Lemma 2.2 we obtain the claimed design.

We can also choose U as a subgroup of index 10 in H. Then U has one orbit of size 2 and all other orbits are regular. Then $k = 6x + 2$. The proof of this case is similar to the previous case.

d) H has one orbit of size 30, and all other orbits of size 60. We choose as U one of the subgroups isomorphic to D_3, D_5, A_4 of H. Then we assemble a block from an orbit of U on the A_5-orbit of length 30 and an orbit of length $|U|$ from each regular A_5-orbit according to Lemma 2.4. So, the block sizes are $3 + 6x, 5 + 10x, 6 + 12x$, respectively. As a group of automorphisms we choose $PGL(2, p^f)$ which is 3-homogeneous. So, $\lambda = \frac{k(k-1)(k-2)}{|U|}$ gives the claimed parameters. We have to show that U is the full set stabilizer of B in each case.

If $U \cong A_4$ then U is not contained in any dihedral group. So, a minimal overgroup M is isomorphic to A_5 or $PSL(2, q^t)$ for some divisor t of f. If $M \cong A_5$ then M is conjugate to H in $PGL(2, q^f)$. Then H would leave invariant B^g for some $g \in PGL(2, q^f)$. But then U has to leave this B^g also invariant. The action of U shows that $B = B^g$ and, thus, $M = H$. Then M does not leave B invariant. If $M \cong PSL(2, p^t)$ then B decomposes into orbits under $PSL(2, p^t)$. One orbit of $PSL(2, p^t)$ has length $q^t + 1$ and all other orbits are regular. Since $5 \cdot |B| = p^f + 1$ in this case,

$$p^f + 1 = 5(p^t + 1) + 5 \cdot r \cdot (p^t + 1)p^t(p^t - 1)/2$$

and

$$p^f - 1 = 5p^t + 3 + 5 \cdot r \cdot (p^t + 1)p^t(p^t - 1)/2$$

where $p^t - 1$ divides $p^f - 1$. With $p^f - 1 = m \cdot (p^t - 1)$ and $m + 3 = a \cdot p^t$ the factor p^t can be cancelled such that

$$5 + a + 5r(p^t + 1)(p^t - 1) = m.$$

again replacing $m + 3$ by $a \cdot p^t$ yields

$$8 + 5r(p^t + 1)(p^t - 1) = a \cdot p^t - a = a(p^t - 1).$$

So, $p^t - 1$ divides 8. The case $p^t = 9$ has wrong orbit sizes and $p^t = 5$ yields $M \cong A_5$. In the other cases p^t is too small.

Now consider $U \cong D_5$. A possible minimal overgroup A of U leaving B invariant would lie in the dihedral group of order $q - 1$. Its intersection

A with the cycle of order $(q-1)/2$ is a subgroup that acts with two fixed points and semiregular on the remaining points. So, the order of A must divide $\gcd((q-1)/2, k-2) = \gcd(30x+20, 10x+5) = 5$ such that U is the full set stabilizer of B. The result follows from Lemma 2.2.

The case $U \cong D_3$ is similar.

e) H has one orbit of size 30, one orbit of size 12, and all other orbits of size 60. Assemble B from one orbit of U from each H orbit. Then B has two points from the first orbit, 5 points from the second orbit, and 10 point from each other orbit. Therefore, $k = 10x + 7$. The index of $U = D_5$ in H is 6 and U contains a point stabilizer of each orbit of H. In any dihedral group containing U the set stabilizer of B is U if B is chosen appropriately according to Lemma 2.4. Thus, also no overgroup containing a dihedral group as a proper overgroup of U cannot be the set stabilizer of B in $PGL(2, p^f)$. The result follows by Lemma 2.2.

f) H has one orbit of size 20, one orbit of size 30, and all other orbits of size 60. Choose $U \cong D_3$ in H. Then U contains a stabilizer of a point of order 2, another stabilizer of a point of order 3, and the trivial group as the stabilizer of the points in the regular H-orbits. So, the U-orbits have lengths 3, 2, 6 respectively. By Lemma 2.4 and Lemma 2.2 we obtain the claimed designs. ■

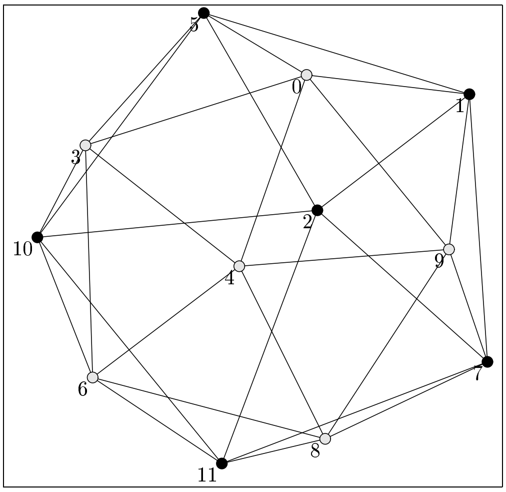
8 Examples

The small Witt design $\mathcal{D}$ with parameters 5-$(12, 6, 1)$ admits $PSL(2, 11)$ as a group of automorphisms. In Table 3 the points of the projective line $PG(1, 11)$ are labels of the vertices of an icosahedron, 11 denoting ∞, such that the rotational automorphisms of the icosahedron induce a permutation group isomorphic to A_5 and which lies in $PSL(2, 11)$. The design consists of a single orbit of $PSL(2, 11)$ on 6-element subsets where the stabilizer U of a block has order 5. We fix a block B having stabilizer U.

There is a subgroup H_1 containing U that is isomorphic to D_5 and which is contained in the overgroup H_2 isomorphic to A_5. A block stabilized by U then corresponds to a 5-ring on the icosahedron together with the point in its center or, resulting in an isomorphic copy of the design, the antipodal of that point. The elements of U fix the chosen point and cyclically permute the points on the 5-ring. It is immediate that the complement of a block again is a block. The dihedral overgroup H_1 interchanges these two orbits of U, since U is a normal subgroup of H_1. Therefore, the design is resolvable by Lemma 2.1. Table 3 visualizes the blocks which lie on an Icosahedron. The other blocks are obtained by translating this set of imprimitivity by the powers of an element of order 11 from $PSL(2, 11)$, e.g. by $(0, 1, \cdots, 10)$.

If we apply Lemma 2.1 to U and H_2 as the full group we obtain another decomposition into 1-$(12, 6, 6)$ designs. If we consider H_2 as the subgroup

Table 3: The Small Witt-Design



H we see that the 5-$(12, 6, 1)$ design is decomposed into 11 parallel classes each being a 1-$(12, 6, 6)$ design. The group $PSL(2, 11)$ has a point stabilizer H_3 of order 55 which also contains U. This time we obtain a decomposition of the 5-$(12, 6, 1)$ design into 12 parallel classes. The classes of the latter two decompositions are no spreads.

We provide generators for some of the subgroups U and H of $PSL(2, p^f)$. We find it conveniant to compute with linear algebra. Therefore we list matrices in $SL(2, p^f)$ that are mapped onto the corresponding elements of $PSL(2, p^f)$ when acting on the set of 1-dimensional subspaces. The kernel of this action is the center Z of $SL(2, p^f)$. Our notation is related to the presentation of the generators of 1-dimensional subspaces as row vectors. Thus, point i of the projective line denotes $< (1, i) >$ for the field element i. The point $\infty =< (0, 1) >$ is denoted by p^f.

Theorem 8.1 *Let $x, y \in GF(p^f)$ such that $x^2 + y^2 = -1$. Then modulo $Z = Z(SL(2, p^f))$ the following matrices generate subgroups of A_4. If 2 is a square, equivalently $16 | p^2 - 1$, then also S_4 is a subgroup of $PSL(2, p^f)$. Otherwise modulo Z the element β below is not contained in $PSL(2, p)$.*

Group	*Generators mod Z*
V_4	$s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, t = \begin{pmatrix} x & y \\ y & -x \end{pmatrix}$
A_3	$\alpha = 1/2 \begin{pmatrix} -x-y-1 & x-y-1 \\ x-y+1 & x+y-1 \end{pmatrix}$
A_4	V_4, A_3
S_4	$A_4, \beta = \begin{pmatrix} x & y+1 \\ y-1 & -x \end{pmatrix}$
D_4	$\begin{pmatrix} y-1 & -x \\ -x & -y-1 \end{pmatrix}, \begin{pmatrix} x & y \\ y & -x \end{pmatrix}$

Conjugating with any element of $PGL(2, p)$ outside $PSL(2, p)$ transforms the subgroups V_4, S_4 of $PSL(2, p)$ into representatives from the other conjugacy class of subgroups if 16 divides $p - 1$.

It is straightforward to verify the claims.

For the embedding of A_5 we refer to the classical approach, see [4, 2, 5].

For $p = 7$ we choose $x = 2$ and $y = 3$. Then the matrices induce permutations on the projective line such that S_4 is the automorphism group of the labelled cube that we used to visualize the 3-$(8, 4, 1)$ design in Table 2 on page 2.

For $p = 23$ we choose $x = 17$ and $y = 20$ and obtain as generators for a subgroup $P \equiv D_4$ from the matrices in Theorem 8.1 the following two permutations on the projective line

$$(0, 10, 21, 20)(1, 4, 3, 14)(2, 7, 9, 6,)(5, 13, 11, 19)(8, 12, 16, 23)(15, 17, 22, 18)$$

$(0, 12)(1, 15)(2, 5)(3, 22)(4, 18)(6, 13)(7, 19)(8, 10)(9, 11)(14, 17)(16, 20)$
$(21, 23)$.

The element α of order 3 above works out as

$$(0, 11, 18)(1, 13, 10)(2, 17, 12)(3, 6, 16)(4, 23, 5)(7, 20, 15)(8, 22, 19)(9, 14, 21).$$

The graph with the points of the projective line as vertices and the edges from the two orbits of $\{0,11\}$ and $\{0,13\}$ under S_4 is a truncated cube. The group acts regularly such that the subgroup of order 8 has 3 orbits of length 8. The three orbits are

$$\{1,3,4,14,15,17,18,22\}\{2,5,6,7,9,11,13,19\}\{0,8,10,12,16,20,21,23\}.$$

Applying α and α^2 yields from each of these sets a spread. The spreads are as follows:

$$\{1,3,4,14,15,17,18,22\},\{0,6,7,12,13,19,21,23\},\{2,5,8,9,10,11,16,20\}$$

$$\{2,5,6,7,9,11,13,19\},\{4,8,10,14,16,17,18,20\},\{0,1,3,12,15,21,22,23\}$$

$$\{0,8,10,12,16,20,21,23\},\{1,2,3,5,9,11,15,22\},\{4,6,7,13,14,17,18,19\}.$$

Their orbits under $PSL(2,23)$ form resolvable 3-$(24,8,21)$ designs.

The matrix

$$\begin{pmatrix} 1 & 6 \\ 6 & 7 \end{pmatrix}$$

induces the odd permutation

$$(0,6,10,2,21,7,20,9)(1,15,4,17,3,22,14,18)(5,8,13,12,11,16,19,23)$$

which leaves the first spread invariant and exchanges the other two. The latter two orbits form disjoint 5-$(24,8,1)$ Witt designs, as can be seen by the arguments in [1]. For one of these we then show in Table 4 the decomposition of the point set into disjoint blocks from the same orbit for the 5-$(24,8,1)$ Witt design.

The big Witt design [14] with parameters 5-$(24,8,1)$ is known to be resolvable, for a deep investigation of the various kinds of decompositions into parallel classes see the paper by Kramer, Magliveras, and Mesner [8]. While these authors make full use of the rich automorphism group M_{24} we use $PSL(2,23)$ only.

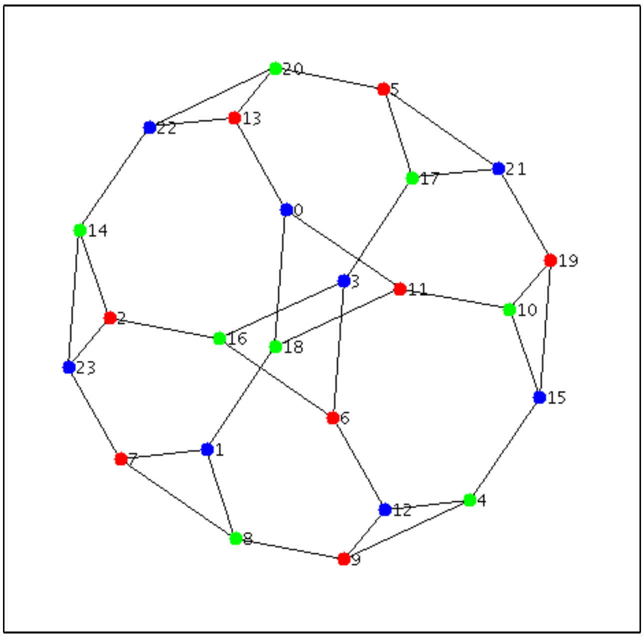
We now consider block size 6. Then a parallel class has to consist of 4 blocks. We first consider an orbit with stabilizer $U \equiv C_6$ and $H \equiv S_4$. The matrices

$$\begin{pmatrix} 21 & 5 \\ 18 & 16 \end{pmatrix}, \begin{pmatrix} 22 & 9 \\ 10 & 1 \end{pmatrix}$$

induce the permutations
$(0,9,12,15,1,20,2,18,23,6,22,4)(3,5,19,21,11,17,14,8,16,10,7,13)$,
$(0,14)(1,19)(2,3)(4,8)(5,20)(6,10)(7,23)(9,17)(11,12)(13,18)(15,21)$
$(16,22)$
that generate H. The square of the first permutation has order 6 and generates U. As a block stabilized by U we choose

$$\{0,12,1,2,23,22\}.$$

Table 4: The Big Witt-Design



Its orbit under H is the spread
$\{0, 12, 1, 2, 23, 22\}$, $\{9, 15, 20, 18, 6, 4\}$, $\{14, 11, 19, 3, 7, 16\}$,
$\{17, 21, 5, 13, 10, 8\}$.
The orbit under $PSL(2, 23)$ is a resolvable 3-$(24, 6, 10)$ design.

We now also consider a stabilizer U of order 2, generated by the permutation
$(0, 2)(1, 22)(3, 14)(4, 20)(5, 8)(6, 15)(7, 11)(9, 18)(10, 21)(12, 23)(13, 17)$
$(16, 19)$
induced by

$$\begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix}.$$

This subgroup lies in a dihedral group H_1 generated by the permutations
$(0, 15, 2, 6)(1, 18, 22, 9)(3, 21, 14, 10)(4, 12, 20, 23)(5, 11, 8, 7)(13, 19, 17, 16)$,
$(0, 10)(1, 17)(2, 21)(3, 6)(4, 7)(5, 23)(8, 12)(9, 16)(11, 20)(13, 22)(14, 15)$
$(18, 19)$
corresponding to the action of the matrices

$$\begin{pmatrix} 2 & 7 \\ 16 & 18 \end{pmatrix}, \begin{pmatrix} 1 & 10 \\ 9 & 22 \end{pmatrix}$$

on the projective line. It turns out that U is the full set stabilizer of

$$\{1, 3, 12, 14, 22, 23\},$$

which is mapped onto disjoint blocks under H_1. The orbit is a resolvable 3-$(24, 6, 30)$ design.

The stabilizer U is contained in another dihedral group H_2 as a complement of a cyclic subgroup of order 4 generated by the permutation action of

$$\begin{pmatrix} 2 & 2 \\ 14 & 3 \end{pmatrix}$$

inducing the permutation

$$(0, 1, 19, 7)(2, 11, 16, 22)(3, 6, 12, 17)(4, 5, 21, 9)(8, 20, 18, 10)(13, 23, 15, 14).$$

The block $\{1, 5, 8, 12, 22, 23\}$ has stabilizer U and is mapped onto disjoint blocks under H_2. The orbit is another resolvable 3-$(24, 6, 30)$ design.

These three orbits of $PSL(2, 23)$, see Table 5, form one of the three 5-$(24, 6, 1)$ designs found by Denniston [3]. So, this design is resolvable.

The other two Steiner 5-$(24, 6, 1)$ designs also each consist of three orbits, both containing the block orbit with representative

$$\{3, 6, 9, 11, 16, 20\}$$

whose stabilizer is some S_3 contained in S_4. The permutation

$$(0, 15, 2, 6)(1, 18, 22, 9)(3, 21, 14, 10)(4, 12, 20, 23)(5, 11, 8, 7)(13, 19, 17, 16)$$

in S_4 maps the block onto 4 disjoint blocks. So, this orbit decomposes into parallel classes.

The other orbits of the two designs have a stabilizer of order 2. Representatives stabilized by the specified C_2 are

$$\{3, 6, 12, 14, 15, 23\}, \{4, 5, 8, 12, 20, 23\}$$

in the first case and

$$\{4, 12, 13, 17, 20, 23\}, \{6, 7, 11, 12, 15, 23\}$$

in the second case. It is not known whether the orbits of these blocks also decompose into parallel classes.

An example of a resolvable 3-design of projective type is a resolvable 3-$(28, 7, 35)$ design. There exists another resolvable 3-$(28, 7, 15)$ design with this group of automorphisms by Theorem 3.2. The 5-$(28, 7, 1)$ design of Denniston [3] is assembled from two orbits of $PSL(2, 27)$ which are 3-$(28, 7, 15)$ and 3-$(28, 7, 35)$ designs. Unfortunately, the 3-$(28, 7, 35)$ design there is not of our projective type such that this Denniston design is not shown to be resolvable.

The smallest example for the case $p^f + 1 = x60 + 42$ is a resolvable 3-$(102, 17, 204)$ design. The symmetries of A_5 in its action on the three

Table 5: Three Resolvable 3-Designs Forming a 5-(24, 6, 1) Design

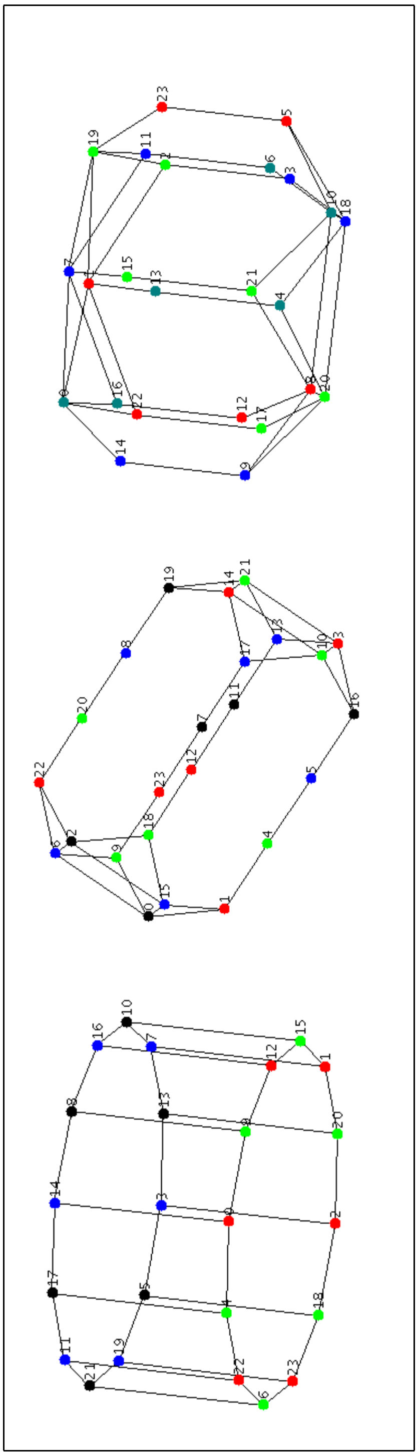
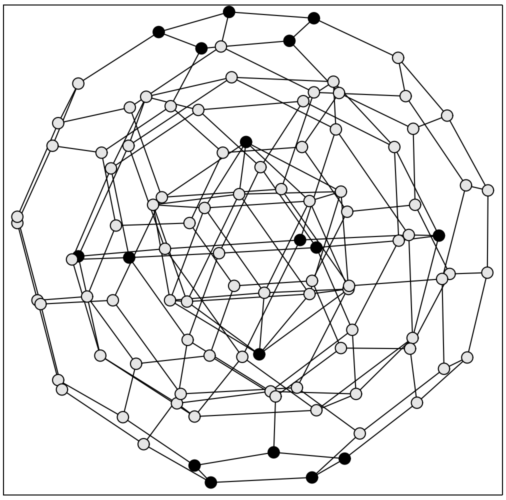


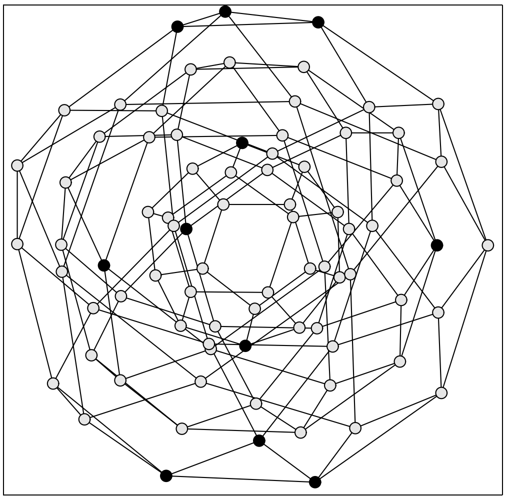
Table 6: A 3-(102,17,408) Design from PGL(2,101)



orbits can be visualized by solids derived from the Icosahedron. The orbit on 12 points is shown on the Icosahedron itself. By choosing as new vertices the centers of the edges and connecting them by an edge if the edges are incident and lie on the boundary of a common face one obtains a solid with 30 vertices. The permutation representation of A_5 on the orbit of length 30 happens to be equivalent to the automorphism group of this solid. The third solid is the well known Bucky-ball, obtained as the truncated Icosahedron. Again, the action on the orbit of size 60 is equivalent to the automorphism group of the Bucky-ball. We visualize the parallel action of A_5 on these three solids by superposition of the solids as spheres with a common center in Table 6.

We give permutation representations of generators of $H \cong A_5$ as a sub-

Table 7: A 3-(110,11,165) Design from PGL(2,109)



group of $PSL(2,101)$, constructed by DISCRETA.

The group H is generated by
$(2,37,85,96,88)(3,73,68,90,74)(4,8,51,84,60)(5,44,34,78,46)$
$(6,80,17,72,32)(7,15,101,66,18)(9,87,67,54,91)(10,22,50,48,77)$
$(11,58,33,42,63)(12,94,16,36,49)(13,29,100,30,35)(14,65,83,24,21)$
$(19,43,99,95,52)(20,79,82,89,38)(23,86,31,71,97)(25,57,98,59,69)$
$(26,93,81,53,55)(27,28,64,47,41)(39,56,62,76,75)(40,92,45,70,61)$,

$(0,40)(1,12)(2,91)(3,76)(4,77)(5,29)(6,97)(7,62)(8,69)(9,96)(10,44)$
$(11,72)(13,22)(14,99)(15,65)(16,45)(17,54)(18,73)(19,89)(20,46)(21,41)$
$(23,53)(24,98)(25,48)(26,63)(27,57)(28,50)(30,52)(31,87)(32,55)(33,86)$
$(34,60)(35,64)(36,70)(37,80)(38,100)(39,59)(42,81)(43,101)(47,95)$
$(49,94)(51,75)(56,83)(58,67)(61,92)(66,82)(68,79)(71,85)(74,84)(78,90)$,

$(0,1)(2,26)(3,64)(4,43)(5,83)(7,22)(8,19)(9,42)(10,15)(11,54)(12,40)$
$(13,62)(14,34)(16,70)(17,72)(18,50)(20,98)(21,78)(23,71)(24,46)(25,82)$
$(27,68)(28,73)(29,56)(30,75)(31,86)(32,80)(33,87)(35,76)(36,45)(37,55)$
$(38,59)(39,100)(41,90)(44,65)(47,74)(48,66)(49,92)(51,52)(53,85)(57,79)$
$(58,67)(60,99)(61,94)(63,91)(69,89)(77,101)(81,96)(84,95)(88,93)$,

$(0,45,92)(1,16,94)(2,37,87)(3,4,46)(5,82,74)(6,93,58)(7,90,89)$
$(8,22,78)(9,85,72)(10,51,57)(11,81,53)(12,36,61)(13,41,19)(14,28,59)$
$(15,75,68)(17,96,23)(18,38,99)(20,35,43)(21,69,62)(24,76,101)$
$(25,84,56)(26,80,86)(27,65,52)(29,48,47)(30,79,44)(31,63,55)$
$(32,33,91)(34,50,100)(39,60,73)(40,70,49)(42,71,54)(64,77,98)$
$(66,95,83)(67,97,88)$.

The first and the third generator generate a subgroup U isomorphic to D_5. It has an orbit $\{0,1\}$ of length 2 on the orbit of length 12 of H, an orbit $\{6,17,32,72,80\}$ of length 5 on the orbit of length 30 of H, and an orbit $\{4,8,19,43,51,52,60,84,95,99\}$ of length 10 on the orbit of length 60 of H. The orbit of this block under $PSL(2,101)$ can be computed from the permutation representation of this group.

The group $PSL(2,101)$ is generated by
$(1,94,86,78,70,62,54,46,38,30,22,14,6,99,91,83,75,67,59,51,43,35,27,$
$19,11,3,96,88,80,72,64,56,48,40,32,24,16,8,101,93,85,77,69,61,53,45,$
$37,29,21,13,5,98,90,82,74,66,58,50,42,34,26,18,10,2,95,87,79,71,63,$
$55,47,39,31,23,15,7,100,92,84,76,68,60,52,44,36,28,20,12,4,97,89,81,$
$73,65,57,49,41,33,25,17,9)$,

$(0,2,52,35,77,82,18,30,39,46,92,47,60,71,66,28,20,7,74,17,97,78,24,$
$23,81,98,36,16,84,8,65,89,61,50,4,27,88,72,9,58,49,70,90,48,63,10,$
$12,44,41,34,100,3,69,62,59,91,93,40,55,13,33,54,45,94,31,15,76,99,$
$53,42,14,38,95,19,87,67,5,22,80,79,25,6,86,29,96,83,75,37,32,43,56,$
$11,57,64,73,85,21,26,68,51,101)$.

The construction of a block in the proof starts from a subgroup D_5 and chooses the two fixed points of C_5 on the Icosahedron. These two determine the axis around which C_5 is rotating. So, we choose an orbit of 5 points of D_5 from the equator of the second solid orthogonal to this axis. The last 10 points are chosen from the two opposite 5-cycles bounding the two faces that are incident with the axis of the rotations in C_5.

Also a resolvable 3-$(110,11,165)$ resulting from the case $v = 1 \times 60 + 30 + 20$ is displayed in Table 7. In this case we use the Dodecahedron and two solids derived from it for our visualization. The first one is obtained by choosing as new vertices the centers of the edges and connecting them by an edge if the edges follow each other on a boundary of a face. The result happens to be isomorphic to that one derived from the Icosahedron by the same operation. The second solid is the truncated Dodecahedron.

The construction of the point set is analogous to the preceding case only replacing C_5 by C_3 and D_5 by D_3 in this case.

Acknowledgements

The author thanks Jumela Sarmiento for stimulating discussions on resolvable designs while she visited the University of Bayreuth and Jean Doyen for pointing out that the small Witt-design can be visualized on the Icosahedron.

References

[1] Th. Beth, D. Jungnickel, H. Lenz: Design Theory. Second edition, Cambridge Univ. Press, 1999.

[2] W. Burnside: Theory of groups of finite order. Second edition Cambridge 1911 (reprint Dover Publ. 1955).

[3] R. H. F. Denniston: Some new 5-designs. *Bull. London Math. Soc.* **8** (1976), 263-267.

[4] L. E. Dickson: Linear groups with an exposition of the galois field theory. Teubner 1901, Leipzig (reprint Dover Publ. 1958, New York).

[5] B. Huppert: *Endliche Gruppen I.* Springer Grundlehren der mathematischen Wissenschaften Bd **134**, (1967).

[6] B. Kaski, L. B. Morales, P. R. J.Ostergard, D. A. Rosenblueth, and C. Velarde Classification of Resolvable 2-(14,7,12) and 3-(14,7,5) Designs. To appear in *J. Comb. Math. and Comb. Comp.*.

[7] A. Kohnert, R. Laue: GRAPH Database. btm2xg.mat.uni-bayreuth.de/GRAPHDB/

[8] E. S. Kramer, S. S. Magliveras, D. M. Mesner: Some resolutions of $S(5,8,24)$. *J. Comb. Theory A* **29** (1980), 166-173.

[9] R. Laue: Eine konstruktive Version des Lemmas von Burnside. *Bayreuther Math. Schr.* **28** (1989), 111-125.

[10] R. A. Liebler, S. S. Magliveras, S. V. Tsaranov Block transitive resolutions of t-designs and Room rectangles. *J. for Statist. Planning and Inference* **58** (1997), 119-133.

[11] J. Sarmiento: Resolutions of $PG(5,2)$ with point-cyclic automorphism group. *J. Comb. Des.* **8** (2000), 2-14.

[12] Tran van Trung: Recursive constructions for 3-designs and resolvable 3-designs. *J. Statist. Planning and Inference* **95** (2001), 341-358.

[13] Tran van Trung: Construction of 3-designs using parallelism. *J. Geom.* **67** (2000), 223-235.

[14] E. Witt: Die 5-fach transitiven Gruppen von Mathieu. *Abh. Math. Seminar Univ. Hamburg* **12** (1938), 256-264.