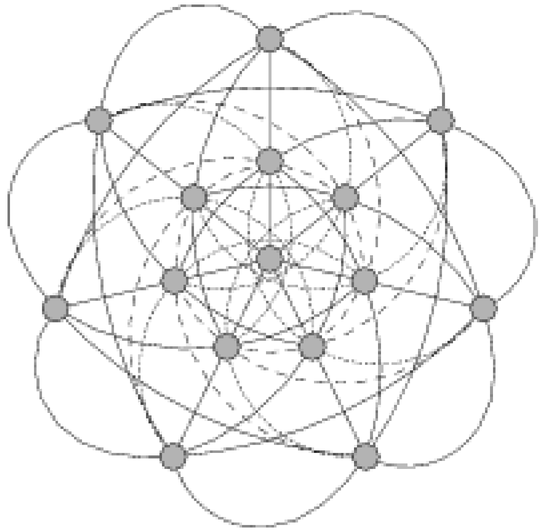


Intersection Numbers of Designs

Anton Betten

March 21, 2000

Address of the author:

Anton Betten
Universität Bayreuth
Lehrstuhl II für Mathematik
95440 Bayreuth

email: Anton.Betten@uni-bayreuth.de

WWW: http://www.mathe2.uni-bayreuth.de/betten/anton.html

A thesis accepted by the Faculty of Mathematics and Physics of the University of Bayreuth for the degree of Doctor of Science.

The German version of this text appeared in Bayreuther Mathematische Schriften **58** (2000), x:1–131.

Contents

1 Introduction **1**

1.1 Incidence Structures and t-Designs 1

1.2 Parameters of t-Designs 5

1.3 Partitions and their Combinatorics 11

2 Intersection Numbers of Designs **31**

2.1 Ordinary Intersection Numbers 32

2.2 Intersection Numbers of Higher Order 34

2.3 Global Intersection Numbers 42

3 The Construction of Designs **49**

3.1 The Method of Kramer and Mesner 49

3.2 Construction of 8-(31, 10, λ) Designs 57

3.3 List of t-Designs with Large t 64

4 The Plesken Ring **69**

4.1 Groups Acting on Lattices 69

4.2 The Plesken Ring 78

4.3 Groups Acting on Ranked Lattices 83

4.4 Acting on the Subset Lattice 91

5 Classification of Designs **97**

5.1 The Computation of Intersection Numbers 97

5.2 Classification of 8-(31, 10, λ) Designs 108

Bibliography **119**

Index **123**

Chapter 1

Introduction

In this chapter, we discuss some basic properties of designs and their parameters. For further study, I recommend the books of van Lint and Wilson [27] and of Cameron and van Lint [8]. Facing only the theory of designs and incidence structures, there are also the books by Beth, Jungnickel and Lenz [2] and the famous book by Dembowski [10].

1.1 Incidence Structures and t-Designs

An *incidence structure* is a system $\mathcal{B}$ of subsets of a set $\mathcal{V}$ whose elements are called *points*. The subsets are called *blocks*. An incidence structure is called *finite*, if the set $\mathcal{V}$ is finite. In this work all incidence structures will be finite. The number of points is denoted by v, the number of blocks is abbreviated by the letter b.

The *incidence relation* is the relation of inclusion between points and blocks. We call a point $p \in \mathcal{V}$ and a block $B \in \mathcal{B}$ *incident* if $p \in B$ holds. An incident point / block pair (p, B) is called *flag*. A non incident point / block pair (p, B) is called *anti flag*. The relation of inclusion and therefore the incidence structure itself is often coded by a matrix, the *incidence matrix*. Let $p_1, \ldots, p_v$ be the points and $B_1, \ldots, B_b$ be the blocks of the incidence structure. The incidence matrix is the $(v \times b)$-matrix $\mathcal{N} = (n_{i,j})$ with $n_{i,j} = 1$ if $p_i \in B_j$ and zero otherwise. On the other hand, every 0/1-matrix $\mathcal{N} = (n_{i,j})$ of size $v \times b$ defines an incidence structure $(\mathcal{V}, \mathcal{B})$ with v points and b blocks. We take v points and b blocks corresponding to the rows and columns of the matrix $\mathcal{N}$, respectively. The point p_i is contained in the block B_j if and only if $n_{i,j} = 1$.

A t-(v, k, λ) *design* is a incidence structure $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ with

(i) $|\mathcal{V}| = v$,

(ii) $|B| = k$ for each block $B \in \mathcal{B}$,

(iii) For each t-subset $T \subseteq \mathcal{V}$ there are exactly λ blocks of $\mathcal{B}$ containing T. In other words: $\forall T \in \binom{\mathcal{V}}{t} : \ \exists_\lambda B \in \mathcal{B} : \ T \subseteq B$.

The numbers t, v, k and λ are (amoung others) the *parameters* of the design. The number t describes the *point regularity*. The number k is the *block size*, λ is the *index* of the design. Not every parameter set belongs to a design. On the other hand, the may exist several designs for the same parameter set. Two designs $\mathcal{D}_1 = (\mathcal{V}, \mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{V}, \mathcal{B}_2)$ are called *isomorphic*, if there exists a permutation $\pi \in \mathrm{Sym}_{\mathcal{V}}$, mapping the set system $\mathcal{B}_1$ onto the set system $\mathcal{B}_2$. Here, application of the permutation π is understood element-wise, i. e. $\mathcal{B}_1^\pi = \{B^\pi \mid B \in \mathcal{B}_1\}$ mit $B^\pi = \{p^\pi \mid p \in B\}$. The relation of isomorphism is an equivalence relation. The isomorphisms of one design onto itself are called *automorphisms*. They form a group with respect to the composition of mappings. This group is called *automorphism group of the design*. A design with $\lambda = 1$ is called *Steiner system*. In a design with point regularity $t \geq 1$, the number of blocks containing a fixed point is a constant

$$r = |\{B \in \mathcal{B} \mid p \in B\}|$$

for $p \in \mathcal{V}$, the *replication number*.

The starting point for the development of design theory may be seen in the following problem of schoolgirls which was posed by Reverend Kirkman (1806-1895) around 1850 (cf. [14], [16], [15]):

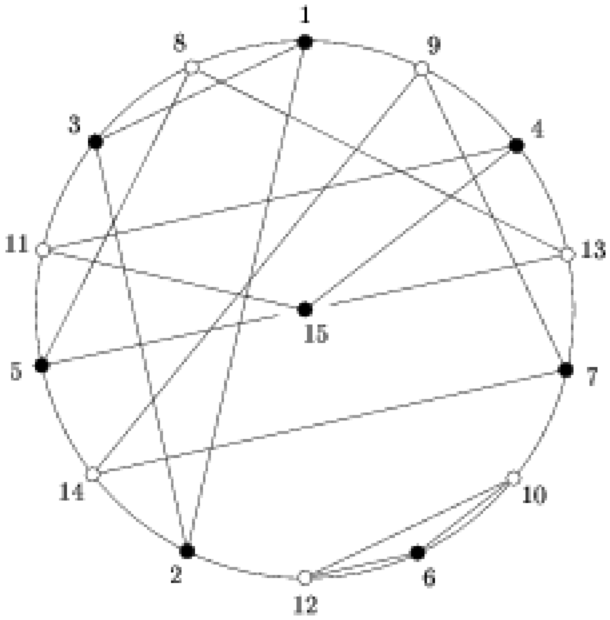
> "*Fifteen young ladies in a school walk out three abreast for seven days in succession; it is required to arrange them daily, so that no two will walk twice abreast.*"

Labelling the 15 schoolgirls by the numbers 1 to 15, we are asked to define 7 times 5 groups or blocks of size three out of the 15 numbers such that all 15 numbers appear in the 5 blocks and any two numbers together do not occur twice in the set of all blocks. The necessary condition $\binom{15}{2} = 105 \geq 7 \cdot 5 \cdot \binom{3}{2}$ is satisfied with equality, so any two numbers occur exactly once together in a block. This means that we are looking at a design on 15 points mit blocksize 3 and the property that any two points ($t = 2$) occur exactly once ($\lambda = 1$) together in a block. The design has the parameters 2-$(15, 3, 1)$ and thus is a Steiner system.

A solution to the schoolgirl problem is shown in Figure 1.1. Following an idea of Beth, Jungnickel, Lenz [2], the fifteen girls are identified with nodes labelled by the numbers 1 to 15. These nodes are placed on the periphery of a circle (with one point in the center of the circle). The three groups of one day's walk are indicated as triangles. The solutions for the other 6 days are obtained by rotating the picture around the central point along the circle in steps of size two. Below the solution for all seven days is displayed in form of a table.

The question whow designs can be constructed has no universal solution. A method for constructing designs will be presented and discussed later in this work. This method qorks well even for large parameters, i. e. high point regularity. Foremost we are interseted in answering the second question which is the following:

> *Given a set of designs fir the same parameter set and on the same set of points $\mathcal{V}$. Determine the isomorphism classes of the designs, i. e.*



Mo			Di			Mi			Do			Fr			Sa			So		
1	2	3	3	6	5	5	7	2	2	4	6	6	1	7	7	3	4	4	5	1
6	10	12	7	13	10	4	9	13	1	8	9	3	11	8	5	14	11	2	12	14
7	9	14	4	8	12	1	11	10	3	14	13	5	12	9	2	10	8	6	13	11
5	8	13	2	11	9	6	14	8	7	12	11	4	10	14	1	13	12	3	9	10
4	11	15	1	14	15	3	12	15	5	10	15	2	13	15	6	9	15	7	8	15

Figure 1.1: A Solution to the Schoolgirl Problem

the classes of designs which are pairwise isomorphic is the above sense.

1.2 Parameters of t-Designs

In this section we recall some basic results on the parameters of designs. A first important observation is that any t-design is at the same time also a $(t-1)$-design. Inductively, it is an s-design for all $0 \le s \le t$:

1.2.1 Lemma *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design and let s be an integer with $0 \le s \le t$. Then $\mathcal{D}$ is also an s-(v, k, λ_s) design with*

$$\lambda_s = \lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} \tag{1.1}$$

(i. e. $\lambda_t = \lambda$).

Putting $s = 0$, we obtain

$$\lambda_0 = \lambda \frac{\binom{v}{t}}{\binom{k}{t}} = b, \tag{1.2}$$

for any t-design, as every block contains the empty set.

In any 1-design (so in any t-design with $t \ge 1$) the number of blocks containing a fixed point is uniquely determined. We put $\lambda_1 = r$ and get from Lemma 1.2.1:

$$vr = kb \ \big(\Leftrightarrow \ \lambda_0 = \lambda_1 \frac{v}{k} \big). \tag{1.3}$$

In any 2-design (so in any t-design with $t \ge 2$) we have

$$\lambda_1 = r = \lambda_2 \frac{\binom{v-1}{2-1}}{\binom{k-1}{2-1}} \ \big(\Leftrightarrow \ r(k-1) = \lambda_2(v-1) \big). \tag{1.4}$$

If we regard a t-(v, k, λ) design $\mathcal{D}$ as a $(t-1)$-design, i. e. more preciesely as a $(t-1)$-(v, k, λ_{t-1}) design, we call it the *design with respect to smaller t* and write red $\mathcal{D}$ (reduced t) For $i \leq t$, $\mathrm{red}^i\,\mathcal{D} = \underbrace{\mathrm{red}\,\mathrm{red}\,\ldots\,\mathrm{red}}_{i\ \mathrm{mal}}\,\mathcal{D}$ is a $(t-i)$-(v, k, λ_{t-i}) design.

The existence of some special t-designs is so obvious that we consider them as *trivial designs*. First of all, we always have the *complete design* holding all k-subsets, i. e. $\mathcal{B} = \binom{\mathcal{V}}{k}$. This design is a t-$(v, k, \lambda_{\max}(v, t, k))$ design with

$$\lambda_{\max}(v, t, k) = \binom{v-t}{k-t}.$$

The integer $\lambda_{\max}(v, t, k)$ is the largest possible index which a design with fixed parameters t, v and k can have.

Another trivial design is the *empty design* without blocks. There is also the one-block design with $k = v$ and $\lambda = 1$. The design with $t = k = 1$ and $\mathcal{V} = \binom{\mathcal{V}}{1} = \mathcal{V}$ is another trivial Steiner System. The design with $k = v - 1$ and $\mathcal{B} = \binom{\mathcal{V}}{v-1}$ is also trivial. Note that the last three examples all describe complete designs.

There are some ways to construct t-designs from other t-designs. Let always $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. At first, the *supplementary design* supp $\mathcal{D}$ has the k-subsets as blocks which do not belong to $\mathcal{B}$. It has the parameters

$$t-(v, k, \lambda_{\max}(v, t, k) - \lambda).$$

As every design admits the supplementary design of index $\lambda_{\max}(v, t, k) - \lambda$, we may require our design to have an index which is at most $\frac{1}{2}\lambda_{\max}(v, t, k)$. The supplementary design of the complete design is the empty design.

Another design is the *complementary design* $\mathcal{D}^c$, which has as blocks the sets $B^c = \mathcal{V} \setminus B$ where B runs through the set of blocks of $\mathcal{D}$. Later we will see that the complementary design is again a t-design and we will compute its index in Corollary 1.2.6. As the complementary design has blocks of size $v - k$, we may require that the designs we are looking at have blocksize at most $\frac{1}{2}v$. The designs with $t = k = 1$ and $k = v - 1$ mentioned above are complementary designs. The complementary design of the one-block design has the empty set as a single block.

For a given parameter set, there does not always exist a design. A useful test for verifying whether a putative design parameter set is realizable is the following:

If a t-(v, k, λ) design exists, then all parameters λ_s of (1.1) must be integral. Thus, for $0 \leq s \leq t$, all denominators in

$$\lambda_s = \lambda \frac{[v - s]_{t-s}}{[k - s]_{t-s}}$$

must divide the corresponding numerators including λ. Here, $[a]_b$ is the *falling factorial* of length b defined as

$$[a]_b := a \cdot (a - 1) \cdots (a - (b - 1))$$

(with $[a]_0 = 1$). A parameter set t-(v, k, λ) is called *admissible* if all λ_s are integral. Let $\Delta\lambda$ be the smallest positive integer such that

$$\frac{\Delta\lambda \cdot [v - s]_{t-s}}{[k - s]_{t-s}}$$

is an integer for all s with $0 \leq s \leq t$. Then all parameter sets of the form t-$(v, k, h \cdot \Delta\lambda)$ with $h \in \mathbb{N}$ are admissible.

Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. For $p \in \mathcal{V}$, let

$$\operatorname{der}_p \mathcal{D} = (\mathcal{V}, \mathcal{B}_p) \ \text{ with } \ \mathcal{B}_p = \{B \setminus \{p\} \mid B \in \mathcal{B},\, p \in B\}$$

be the *derived design*. In addition, we call

$$\operatorname{res}_p \mathcal{D} = (\mathcal{V}, \mathcal{B}^p) \ \text{ with } \ \mathcal{B}^p = \{B \in \mathcal{B} \mid p \notin B\}$$

the *residual design* of $\mathcal{D}$.

1.2.2 Lemma *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design and let $p \in \mathcal{V}$ be an arbitrary point. Then* *(i)* $\operatorname{der}_p \mathcal{D}$ *is a*

$$(t-1)-(v-1, k-1, \lambda)$$

design,

(ii) $\operatorname{res}_p \mathcal{D}$ *is a*

$$(t-1)-(v-1, k, \lambda_{t-1}-\lambda)$$

design, with $\lambda_{t-1}-\lambda = \lambda\frac{v-k}{k-(t-1)}$.

Figure 1.2 shows the relation between the parameters of design and the parameters of the dreived and residual designs and the design with respect to smaller t.

$$\begin{tikzcd}
 & t\text{-}(v,k,\lambda) \arrow[dl, "\mathrm{red}"'] \arrow[d, "\mathrm{der}"] \arrow[dr, "\mathrm{res}"] & \\
(t-1)\text{-}(v,k,\lambda\frac{v-(t-1)}{k-(t-1)}) & (t-1)\text{-}(v-1,k-1,\lambda) & (t-1)\text{-}(v-1,k,\lambda\frac{v-k}{k-(t-1)})
\end{tikzcd}$$

Figure 1.2: The Parameters of the Designs $\mathcal{D}$ and red $\mathcal{D}$, der $\mathcal{D}$ and res $\mathcal{D}$

The following counting principle is a useful combinatorial method. Before stating the result, we present a small example. Let Ω be a finite set and let A, B and C be arbitrary subsets of Ω. Assume we want to determine the cardinality of the set $\hat{\Omega} = \Omega \setminus (A \cup B \cup C)$ using only the cardinalities of Ω and of all intersections of the sets A, B and C. Then, according to Figure 1.3,

$$|\hat{\Omega}| = |\Omega| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|.$$

The general case is settled by the following lemma:

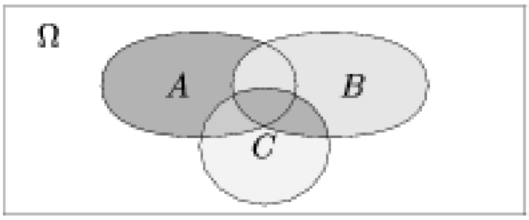


Figure 1.3: Computing $|\hat{\Omega}|$ using Inclusion / Exclusion

1.2.3 Lemma *(Principle of Inclusion / Exclusion or Sieve Formula) Let Ω be a finite set and let $A_1, \ldots, A_\ell$ be a set of subsets of Ω. Let $\hat{\Omega} = \Omega \setminus \bigcup_{i=1}^{\ell} A_i$ be the set of elements of Ω which are contained in none of the sets $A_1, \ldots, A_\ell$. Then*

$$|\hat{\Omega}| = |\Omega| + \sum_{j=1}^{\ell} (-1)^j \sum_{\substack{M \in \binom{\{1,\ldots,\ell\}}{j}, \\ M = \{m_1,\ldots,m_j\}}} \left| \bigcap_{k=1}^{j} A_{m_k} \right| .$$

1.2.4 Lemma *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. For $i, j \in \mathbb{N}$ with $i + j \leq t$, let $I \in \binom{\mathcal{V}}{i}$ and $J \in \binom{\mathcal{V}}{j}$ be disjoint subsets of $\mathcal{V}$. Then the number*

$$\lambda_{i,j} = \Big| \{B \in \mathcal{B} \mid I \subseteq B, B \cap J = \emptyset\} \Big|$$

is independent of the choice of the subsets I and J. In addition, $\lambda_{i,0} = \lambda_i$ for all $i \leq t$ and $\lambda_{t,0} = \lambda$. The recursion

$$\lambda_{i,j+1} = \lambda_{i,j} - \lambda_{i+1,j} \tag{1.5}$$

is satisfied for $i + j < t$.

We display the numbers $\lambda_{i,j}$ for $i + j \leq t$ in a triangular scheme as in Figure 1.4. The initial values $\lambda_s = \lambda_{s,0}$ for $0 \leq s \leq t$ together with (1.5) allow the computation of all values. Other, direct formulae are the following:

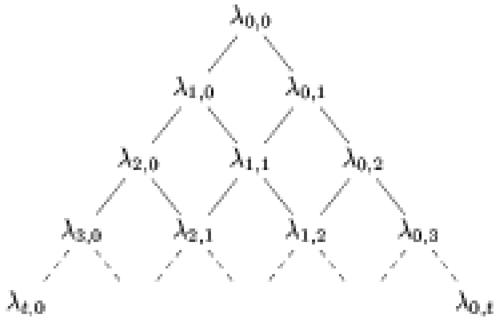


Figure 1.4: The Parameters $\lambda_{i,j}$ of a t-Design

1.2.5 Lemma *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. Let I and J be disjoint subsets of $\mathcal{V}$ of size i and j, respectively, where $i + j \leq t$. Then,*

(i) $\lambda_{0,j} = \sum_{s=0}^{j} (-1)^j \binom{j}{s} \lambda_s$,

(ii) $\lambda_{i,j} = \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}$ *(Ray-Chaudhuri and Wilson [24]).*

Applying this result to the complementary design of a t-design, we see that this again is a t-design: Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-design and let T be an arbitrary t-subset of $\mathcal{V}$. The blocks of the complementary design $\mathcal{D}^c$ containing T are exactly the complements of blocks of $\mathcal{B}$ avoiding all elements of T. This proves:

1.2.6 Corollary *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. Then the complementary design $\mathcal{D}^c$ is a t-design with parameters*

$$t - (v, v-k, \lambda_{O,t}) \quad \textit{with} \quad \lambda_{0,t} = \lambda \frac{\binom{v-t}{k}}{\binom{v-t}{k-t}} = \lambda \frac{[v-k]_t}{[k]_t}.$$

1.3 Partitions and their Combinatorics

In this section, we present some results of the combinatorics of partitions. Much of this work is inspired by the books of Aigner [1], Halder and Heise [11, Chapter 1, 4 and 5] and Kerber [13].

Let $n \in \mathbb{N}$ be a natural number ($0 \in \mathbb{N}$) and let N be a n-element set. We denote by $(a_1, \ldots, a_r)$ the *sequence* and by $[a_1, \ldots, a_r]$ the *multiset* of elements $a_1, \ldots, a_r$. The elements of the multiset may be freely rearranged and multiplicities are taken into account. In order to simplify notation, we may express multiplicities as exponents. If the multiset consists of natural numbers, we may order the entries according to descending magnitude. We call the multiset $[a_1, \ldots, a_r]$ of natural numbers *in standard form* if $a_1 \geq \ldots \geq a_r$ holds.

A *decomposition* of a set N is a system of possibly empty, pairwise disjoint subsets $\mathscr{P}_1, \ldots, \mathscr{P}_r$ with $\bigcup_{i=1}^r \mathscr{P}_i = N$. A decomposition is *ordered* if the sets form a sequence. Otherwise, we call it *unordered*. In both cases, we write $\mathscr{P} \vdash N$, where $\mathscr{P} = (\mathscr{P}_1, \ldots, \mathscr{P}_r)$ may be either a sequence or a multiset $\mathscr{P} = [\mathscr{P}_1, \ldots, \mathscr{P}_r]$ of pairwise disjoint subsets of the set N. More formally,

$$\mathscr{P} \vdash N \iff \bigcup_{i=1}^{r} \mathscr{P}_i = N \ \wedge \ \mathscr{P}_i \cap \mathscr{P}_j = \emptyset \text{ for } i \neq j$$

for $\mathscr{P} = (\mathscr{P}_1, \ldots, \mathscr{P}_r)$ and $\mathscr{P} = [\mathscr{P}_1, \ldots, \mathscr{P}_r]$, respectively. The possibly empty subsets $\mathscr{P}_i$ are the *parts* of the decomposition.

1.3.1 Example

(i) $(2, 7, 1, 2)$ is the *sequence* and $[2, 7, 1, 2] = [1, 2^2, 7]$ the *multiset* of elements $2, 7, 1, 2$. As we do not consider ordering of the elements of a multiset we have $[2, 7, 1, 2] = [7, 2, 2, 1] = [7, 2^2, 1]$. The last two forms are the standardforms of the multiset.

(ii) The sequence $(\{2,3\},\{1\},\{4\})$ is an ordered decomposition of the set $\{1,2,3,4\}$. The multiset $[\{2,3\},\{1\},\{4\}]$ is an unordered decomposition of the same set.

$\diamond$

Let us now define partitions. There are various kinds of partitions and the terminology not always seems to be consistent in the literature. A *set partition* is a decomposition.

A *number partition* of $n \in \mathbb{N}$ is a sequence $p = (p_1, \dots, p_r)$ or a multiset $p = [p_1, \dots, p_r]$ of natural numbers $p_1, \dots, p_r$ with $\sum_{i=1}^r p_i = n$. The p_i are the *parts* are the parts of the partition and we again write $p \vdash n$:

$$p \vdash n \iff \sum_{i=1}^{r} p_i = n$$

for $p = (p_1, \dots, p_r)$ and $p = [p_1, \dots, p_r]$, respectively.

Alltogether, we are going to introduce 8 different types of partitions, cf. Fig. 1.5. We have 4 set partitions and 4 number partitions, 4 ordered and 4 unordered partitions and finally 4 generalized and 4 proper partitions. Choosing these three properties as labels of the three dimensions of the cube, we obtain the figure.

A number partition $(p_1, \dots, p_r)$ or $[p_1, \dots, p_r]$ is called *proper*, if $p_i \geq 1$ for $i = 1, \dots, r$. If only $p_i \geq 0$ is required, we call it a *generalized number partition* (strictly speaking, the proper partitions thus also belong to the class of generalized partitions).

An ordered number partition is a partition whose parts form a sequence of numbers. in an unordered number partition, the parts form a multiset. An unordered partition is in standard form if the corresponding multiset has this property. The sets of proper unordered, proper ordered, generalized unordered and generalized ordered number partitions of n will be denoted by $\overline{\Pi}(n)$, $\Pi(n)$, $\overline{\Pi}^*(n)$ and $\Pi^*(n)$. More precisely, we have

$$\overline{\Pi}(n) = \{ [p_1, \dots, p_r] \vdash n \mid r \in \mathbb{N},\ \ p_i \in \mathbb{N},\ \ p_i \geq 1 \text{ for } i = 1, \dots, r \},$$

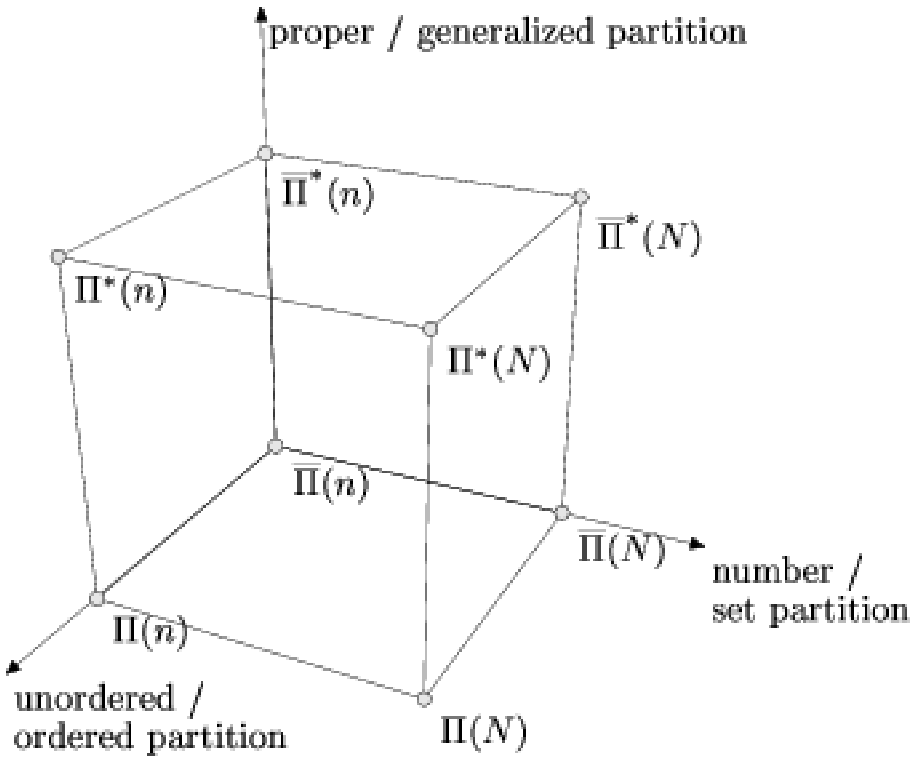


Figure 1.5: The Eight Types of Partitions

$$\Pi(n) = \{\ (p_1, \ldots, p_r) \vdash n \mid r \in \mathbb{N},\ \ p_i \in \mathbb{N},\ \ p_i \geq 1 \text{ for } \ i = 1, \ldots, r\ \},$$
$$\overline{\Pi}^*(n) = \{\ [p_1, \ldots, p_r] \vdash n \mid r \in \mathbb{N},\ \ p_i \in \mathbb{N},\ \ p_i \geq 0 \text{ for } \ i = 1, \ldots, r\ \},$$
$$\Pi^*(n) = \{\ (p_1, \ldots, p_r) \vdash n \mid r \in \mathbb{N},\ \ p_i \in \mathbb{N},\ \ p_i \geq 0 \text{ for } \ i = 1, \ldots, r\ \}.$$

1.3.2 Example [2, 4, 2, 1] is in $\overline{\Pi}(9)$, [4, 2, 2, 1] is this partition in standard form. (2, 4, 2, 1) is in $\Pi(9)$. [2, 4, 2, 0, 1] is in $\overline{\Pi}^*(9)$, [4, 2, 2, 1, 0] is this partition in standard form. (2, 4, 2, 0, 1) is in $\Pi^*(9)$. ◇

For set partitions, we also distinguish four types. A set partition $\mathscr{P} = (\mathscr{P}_1, \ldots, \mathscr{P}_r) \vdash N$ or $\mathscr{P} = [\mathscr{P}_1, \ldots, \mathscr{P}_r] \vdash N$ is called *proper* if $\mathscr{P}_i \neq \emptyset$ for $i = 1, \ldots, r$. A set partition, whose parts may be empty is called *generalized*.

In particular, the class of proper set partitions also belong to the generalized set partitions. The sets of proper unordered, properordered, generalized unordered and generalized ordered set partitions are

$$\begin{aligned}
\overline{\Pi}(N) &:=\{\ [\mathcal{P}_1, \dots, \mathcal{P}_r] \vdash N \mid r \in \mathbb{N},\ \mathcal{P}_i \neq \emptyset \text{ for } i = 1, \dots, r\ \},\\
\Pi(N) &:=\{\ (\mathcal{P}_1, \dots, \mathcal{P}_r) \vdash N \mid r \in \mathbb{N},\ \mathcal{P}_i \neq \emptyset \text{ for } i = 1, \dots, r\ \},\\
\overline{\Pi}^*(N) &:=\{\ [\mathcal{P}_1, \dots, \mathcal{P}_r] \vdash N \mid r \in \mathbb{N}\ \},\\
\Pi^*(N) &:=\{\ (\mathcal{P}_1, \dots, \mathcal{P}_r) \vdash N \mid r \in \mathbb{N}\ \}.
\end{aligned}$$

1.3.3 Example $[\{2, 3\}, \{1\}, \{4\}]$ is an unordered set partition (i. e. belongs to $\overline{\Pi}(\{1, 2, 3, 4\})$), $(\{2, 3\}, \{1\}, \{4\})$ is an ordered set partition (i. e. belongs to $\Pi(\{1, 2, 3, 4\})$), $[\{2, 3\}, \emptyset, \{1\}, \emptyset, \{4\}]$ is an unordered generalized set partition (i. e. belongs to $\overline{\Pi}^*(\{1, 2, 3, 4\})$), $(\{2, 3\}, \emptyset, \{1\}, \emptyset, \{4\})$ is an ordered generalized set partition (i. e. belongs to $\Pi^*(\{1, 2, 3, 4\})$). ◇

The *length* of a partition is the number of parts. We write $\ell(p)$ or $\ell(\mathcal{P})$ for the length of a number partition p or the length of a set partition $\mathcal{P}$. The set of partitions with fixed length r is denoted using the above notation for the partition and indicating the length r in the index. So, $\Pi_r(N)$, $\overline{\Pi}_r(N)$, $\Pi_r(n)$ and $\overline{\Pi}_r(n)$ denote the set partitions (number partitions) of N (of n) with exactly r parts. The overlined partition symbol stands for the unordered versions of the partitions.

For a number partition p, the sum of all parts is the *weight* of p, written as $|p| := \sum_{i=1}^{\ell(p)} p_i$.

Let us consider Fig. 1.5 again. in any of the three dimansions of the three-space, we have a projection mapping. These mappings go in the opposite direction as the arrows indicated in the figure:

(i) We can map every ordered partition onto its unordered form by forgetting about the ordering. Thus we have two maps

$$\bar{\ } : \Pi(N) \to \overline{\Pi}(N),\ \mathcal{P} = (\mathcal{P}_1, \dots, \mathcal{P}_r) \mapsto \overline{\mathcal{P}} = [\mathcal{P}_1, \dots, \mathcal{P}_r],$$

$$\bar{\cdot} : \Pi(n) \to \overline{\Pi}(n),\ p = (p_1, \ldots, p_r) \mapsto \overline{p} = [p_1, \ldots, p_r].$$

(ii) For set partitions, the sizes of the classes form a number partition whose weight is the cardinality of the partitioned set. We consider this number partition as ordered if and only if the original partition was ordered. So, for a set N of cardinality n, we get two maps

$$\|\cdot\| : \Pi(N) \to \Pi(n),\ \mathcal{P} = (\mathcal{P}_1, \ldots, \mathcal{P}_r) \mapsto (|\mathcal{P}_1|, \ldots, |\mathcal{P}_r|),$$
$$\|\cdot\| : \overline{\Pi}(N) \to \overline{\Pi}(n),\ \mathcal{P} = [\mathcal{P}_1, \ldots, \mathcal{P}_r] \mapsto [|\mathcal{P}_1|, \ldots, |\mathcal{P}_r|],$$

which we call the *type maps*.

(iii) We can map any generalized partition onto a proper partition by forgetting about empty sets in set partitions or zero parts in number partitions, respectively. In case that the original partition was an ordered partition, we simply delete the empty parts and keep the ordering of the remaining parts. Thus we have mappings

$$\hat{\cdot} : \Pi^*(N) \to \Pi(N),\ \mathcal{P} \mapsto \hat{\mathcal{P}},$$
$$\hat{\cdot} : \overline{\Pi}^*(N) \to \overline{\Pi}(N),\ \mathcal{P} \mapsto \hat{\mathcal{P}},$$
$$\hat{\cdot} : \Pi^*(n) \to \Pi(n),\ p \mapsto \hat{p},$$
$$\hat{\cdot} : \overline{\Pi}^*(n) \to \overline{\Pi}(n),\ p \mapsto \hat{p}.$$

All three different kinds of mappings play an important role in the proofs of this section.

Set partitions are useful to study mappings between finite sets. Any mapping $f : N \to R$ with $N = \{1, \ldots, n\}$ and $R = \{1, \ldots, r\}$ gives rise to a set partition

$$\mathcal{P}_f = (\mathcal{P}_1(f), \ldots, \mathcal{P}_r(f)) \tag{1.6}$$

of N while putting

$$\mathcal{P}_i(f) := f^{-1}(\{i\}) \text{ for } i = 1, \ldots r.$$

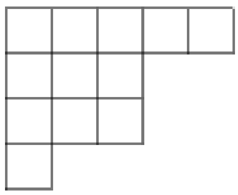
The ordered set partition $\mathcal{P}_f$ describes the mapping f uniquely.

1.3.4 Example The mapping $f : \{1, \dots, 4\} \mapsto \{1, \dots, 5\}$ with $f(1) = 3$, $f(2) = 1$, $f(3) = 1$, and $f(4) = 5$ has associated with it the set partition $\mathcal{P}_f = (\{2, 3\}, \emptyset, \{1\}, \emptyset, \{4\})$. ◇

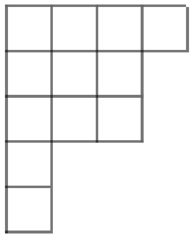
1.3.5 Remark $\mathcal{P}_f$ is proper if and only if f is surjective.

We can consider set partitions and mappings under the action of groups. In particular we have the action of the symmetric groups Sym_N and Sym_R. Acting with Sym_R, we may identify the orbit of a partition $\mathcal{P}_f$ with an unordered partition, i. e. with a multiset. For the corresponding orbit under Sym_N, the type of the partition is an invariant.

It is sometimes useful to draw partitions in form of a diagram, the *Ferrers diagram*. Let $p = [p_1, \dots, p_r]$ be an unordered number partition in standard form. We draw a diagram with boxes aligned in rows and columns. The i-th row represents the part p_i and consists of p_i left aligned boxes. Thus, the partition $p = [5, 3, 3, 1]$ has the diagram



The *conjugate partition* is obtained by reading the diagram column by column. In other words, the conjugate partition is obtained by transposing the Ferrers diagram of the partiton at the diagonal from the upper left corner to the lower right corner. We denote the conjugate partition of p by p'. For the above partition $p = [5, 3, 3, 1]$ we get the transposed Ferrers diagram



describing the conjugate partition $p' = [4, 3, 3, 1, 1]$. Note that the length of the conjugate partition is equal to p_1. The i-th entry of the conjugate partition is the number of parts of p which are of size i or larger:

$$(p')_i = \big|\{j \leq \ell(p) \mid p_j \geq i\}\big|.$$

Let $a = [a_1, a_2, \ldots, a_r]$ be a partition of the number $n \in \mathbb{N}$. The *multinomial coefficient*

$$\binom{n}{a} := \binom{n}{a_1, a_2, \ldots, a_r} := \frac{n!}{\prod_{i=1}^{r} a_i!}$$

is independent of the ordering of the parts of the partition a. The next lemma shows that it is a natural number as it describes the cardinality of a set.

1.3.6 Lemma *Let $a \in \Pi_r(n)$ and let N be an n-element set. The number of possibilities to decompose the set N into r ordered classes of sizes $a_1, \ldots, a_r$ is $\binom{n}{a}$. In other words,*

$$\big|\{\, \mathcal{A} \in \Pi_r(N) \;:\; \|\mathcal{A}\| = a \,\}\big| = \binom{n}{a}.$$

1.3.7 Example The number of ways to write the word MISSISSIPPI in arbitrary order of its letters is

$$\binom{11}{1, 4, 4, 2} = 34650.$$

◇

Our next aim is to determine the number of possibilities to partition an n-element set into unordered classes of prescribed size. Let $[a_1, a_2, \ldots a_{\ell(a)}] \in$

$\overline{\Pi}(n)$ with $a_1 \geq a_2 \geq \ldots \geq a_{\ell(a)}$. The ordered partition

$$\Delta a := (a_1 - a_2, a_2 - a_3 \ldots, a_{\ell(a)-1} - a_{\ell(a)}, a_{\ell(a)}) \in \Pi^*(a_1)$$

is called *difference partition* of a.

1.3.8 Remark Let $a \in \overline{\Pi}(n)$. Then

$$(\Delta a')_i = \left|\{j \leq \ell(a) \mid a_j = i\}\right|.$$

The partition $\Delta a'$ is also called the *cycle type* of a. It is $|\Delta a'| = \ell(a)$ and $\sum_{i=1}^{a_1} i \cdot (\Delta a')_i = |a|$.

1.3.9 Example Take the partition $a = [5, 2, 2, 1]$. The conjugate partition is $a' = [4, 3, 1, 1, 1]$. The cycle type is $\Delta a' = (1, 2, 0, 0, 1) \in \Pi^*(\ell(a))$. Moreover, $1 + 2 \cdot 2 + 1 \cdot 5 = 10 = |a|$. $\diamond$

1.3.10 Lemma *Let $a \in \Pi(n)$ and let N be an n-element set. Let $r = \ell(a)$. The number of possibilities to decompose the set N into unordered classes of size $a_1, a_2, \ldots, a_r$ is*

$$\frac{1}{|\Delta a'|!} \cdot \binom{|\Delta a'|}{\Delta a'} \cdot \binom{|a|}{a}.$$

Proof: According to Lemma 1.3.6, there are $\binom{|a|}{a}$ set partitions $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_r)$ of N with $|\mathcal{A}_i| = a_i$. Then $\overline{\mathcal{A}} = \{\mathcal{A}_1, \ldots, \mathcal{A}_r\}$ is a set partition with unordered classes. According to Remark 1.3.8, every set partition $\mathcal{A}$ with $\|\mathcal{A}\| = a$ has exactly $(\Delta a')_i$ classes of size i. Every permutation mapping these classes to themselves does not change the type $||\mathcal{A}||$ of the partition. All set partitions with the same unordered partition $\overline{\mathcal{A}}$ are obtained by such a permutation of the classes of the partition $\mathcal{A}$. Thus, the number of unordered set partitions of type a equals

$$\frac{1}{\prod_{i=1}^{a_1}(\Delta a')_i!} \cdot \binom{n}{a} = \frac{1}{\ell(a)!} \cdot \binom{|\Delta a'|}{\Delta a'} \cdot \binom{|a|}{a}.$$

$\square$

1.3.11 Example (Continuation of Example 1.3.7) The number of ways to decompose an 11-set into unordered classes of size 4, 4, 2, 1 is

$$\frac{1}{4!}\cdot\binom{4}{1,1,2}\cdot\binom{11}{4,4,2,1}=\frac{1}{2!}\cdot\binom{11}{4,4,2,1}=17325$$

(since $a'=[4,4,2,1]'=[4,3,2,2]$ and $\Delta a'=(1,1,0,2)$). ◇

Often one is interested in the overall number of partitions of an n-element set into r classes (independent of the type of the partition). This number can be determined by noticing that the map $\|\cdot\|$ yields an unordered number partition of n with exactly r classes. Running through all such number partitions, we can obtain the requested number of set partitions by application of Lemma 1.3.10:

1.3.12 Lemma *The number of possibilities to decompose an n-element set N into r unordered classes is*

$$\mathcal{S}_2(n,r):=\frac{1}{r!}\sum_{a\in\overline{\Pi}_r(n)}\binom{r}{\Delta a'}\binom{n}{a}=|\overline{\Pi}_r(N)|.$$

This number is called Stirling number of the second kind.

1.3.13 Example Let us compute $\mathcal{S}_2(5,3)$. There are exactly two partitions of the number 5 into 3 parts: $a=[3,1,1]$ and $b=[2,2,1]$. The conjugate partitions are $a'=[3,1,1]$ and $b'=[3,2]$. Thus, $\Delta a'=(2,0,1)$ and $\Delta b'=(1,2)$. By Lemma 1.3.12, we get

$$\begin{aligned}\mathcal{S}_2(5,3)&=\frac{1}{3!}\left(\binom{3}{2,0,1}\cdot\binom{5}{3,1,1}+\binom{3}{1,2}\cdot\binom{5}{2,2,1}\right)\\&=\frac{1}{6}\cdot(60+90)=25.\end{aligned}$$

◇

Table 1.1 displays the values of $\mathcal{S}_2(n,r)$. The number $B(n)=\sum_{r=0}^{n}\mathcal{S}_2(n,r)$ is called *Bell number*

	$\mathcal{S}_2(n,r), r =$											
n	0	1	2	3	4	5	6	7	8	9	10	$B(n)$
0	1	0	0	0	0	0	0	0	0	0	0	1
1	0	1	0	0	0	0	0	0	0	0	0	1
2	0	1	1	0	0	0	0	0	0	0	0	2
3	0	1	3	1	0	0	0	0	0	0	0	5
4	0	1	7	6	1	0	0	0	0	0	0	15
5	0	1	15	25	10	1	0	0	0	0	0	52
6	0	1	31	90	65	15	1	0	0	0	0	203
7	0	1	63	301	350	140	21	1	0	0	0	877
8	0	1	127	966	1701	1050	266	28	1	0	0	4140
9	0	1	255	3025	7770	6951	2646	462	36	1	0	21147
10	0	1	511	9330	34105	42525	22827	5880	750	45	1	115975

Table 1.1: Stirling Numbers of the Second Kind $\mathcal{S}_2(n,r)$ and Bell Numbers $B(n)$

1.3.14 Lemma *The number of surjective functions of an n-element set N into an r-element set is*

$$r! \cdot \mathcal{S}_2(n,r) = \sum_{a \in \overline{\Pi}_r(n)} \binom{r}{\Delta a'} \binom{n}{a} = \sum_{\substack{a_1 \geq 1, \dots, a_r \geq 1 \\ \sum_{i=1}^r a_i = n}} \binom{n}{a} = |\Pi_r(N)|.$$

Proof: (Cf. Kerber [13, page 81] or Halder and Heise [11, proof of Satz (4.1)]) Let $N = \{1, \dots, n\}$ and $R = \{1, \dots, r\}$ be sets of size n and r. According to Remark 1.3.5, any surjective function $f : N \to R$ defines an ordered proper set partition $\mathcal{A}_f$ of N, whose parts are the preimages of the elements of R under f. Thus $\mathcal{A}_f \in \Pi(N)$. On the other hand, the surjective function f is uniquely determined by the pre-images and thus by the partition $\mathcal{A}_f$. This means that there are as many surjective functions $f : N \to R$ as there are partitions in $\Pi_r(N)$. Now $\bar{\ }$ maps the partitions $\Pi_r(N)$ surjectively onto $\overline{\Pi}_r(N)$ and every unordered partition of $\overline{\Pi}_r(N)$ is the image of exactly $r!$ ordered partitions. Thus by Lemma 1.3.12

$$\mathcal{S}_2(n,r) = |\overline{\Pi}_r(N)| = \frac{1}{r!}|\Pi_r(N)|.$$

Multipying this equation by $r!$ yields equality of the first two and the last terms of the stated equality. In order to verify the correctness of the third term we note that the type of the partition $\mathcal{A}$ is an ordered number partition of n into r parts: $||\mathcal{A}|| = (a_1, \ldots, a_r) \in \Pi_r(n)$, $a_1 \geq 1, \ldots, a_r \geq 1$ and $\sum_{i=1}^r a_i = n$. By Lemma 1.3.6, for each such type there are exactly $\binom{n}{a}$ set partitions of N. □

We denote the number of (unordered) partitions of n into r parts by $P_{n,r}$. The matrix $(P_{n,r})$ is lower triangular with ones on the diagonal. The total number of partitions of the number n is $P_n := \sum_{k=1}^n P_{n,k}$.

1.3.15 Lemma *Let r and n be natural numbers with $1 \leq r \leq n$ and let N be an n-set. Then*

(i) $\left|\Pi_r(N)\right| = r! \cdot \mathcal{S}_2(n,r)$,

(ii) $\left|\Pi_r^*(N)\right| = \sum_{k=1}^r \binom{n}{k} \cdot k! \cdot \mathcal{S}_2(n,k) = r^n$,

(iii) $\left|\overline{\Pi}_r(N)\right| = \mathcal{S}_2(n,r)$,

(iv) $\left|\overline{\Pi}_r^*(N)\right| = \sum_{k=1}^r \mathcal{S}_2(n,k)$,

(v) $\left|\Pi_r(n)\right| = \binom{n-1}{r-1}$,

(vi) $\left|\Pi_r^*(n)\right| = \sum_{k=1}^r \binom{r}{k} \cdot \binom{n-1}{k-1}$,

(vii) $\left|\overline{\Pi}_r(n)\right| = P_{n,r}$,

(viii) $\left|\overline{\Pi}_r^*(n)\right| = \sum_{k=1}^r P_{n,k} = P_n$.

Proof:

(i) Lemma 1.3.14.

(ii) Each partition $\mathcal{A} \in \Pi_r^*(N)$ has a certain number, say k, of nonempty parts. Removing the empty parts, we get the proper partition $\hat{\mathcal{A}}$ of $\Pi_k(N)$. For each such partition, there are exactly $\binom{n}{n-k} = \binom{n}{k}$ ways to place the $n-k$ empty parts to obtain an element of $\Pi_r^*(N)$. Using (i), we get

$$\left|\Pi_r^*(N)\right| = \sum_{k=1}^{n} \binom{n}{k} \left|\Pi_k(N)\right| = \sum_{k=1}^{n} \binom{n}{k} \cdot k! \cdot \mathcal{S}_2(n, k).$$

Every partition of $\Pi_r^*(N)$ can by (1.6) be coded in form of a mapping $f : N \to R = \{1, \dots, r\}$. As we consider generalized partitions, these maps are not necessarily surjective (Remark 1.3.5). Thus there are exactly r^n such functions and this equals the number of elements of $\Pi_r^*(N)$.

(iii) Lemma 1.3.12.

(iv) Follows from (iii).

(v) In the nonnegative part $\mathbb{N} \times \mathbb{N}$ of the integral lattice $\mathbb{Z} \times \mathbb{Z}$, we define for any partition $a \in \Pi_r(n)$ a path leading from the point $(0, 0)$ to the point (r, n). Initially, we put $P_0 = (0, 0)$. For $i = 1, \dots, r$, define new points Q_i and P_i by $Q_i = (i-1, \sum_{j=1}^{i} a_j)$ and $P_i = (i, \sum_{j=1}^{i} a_j)$. The sequence of points $P_0, Q_1, P_1, Q_2, \dots, Q_r, P_r$ defines a path from $P_0 = (0, 0)$ to $P_r = (r, n)$. This path resembles a staircase, where the pairs of points Q_i and P_i together form just one step (cf. Figure 1.6). As all parts of a are nonzero, the height of the points P_i increases strictly. Figure 1.6 shows the staircase obtained from the partition $(1, 2, 1, 1)$. Projecting the y-coordinates of all points $P_1, \dots, P_{r-1}$ onto the y-axis, we obtain an $(r-1)$ subset of the set of numbers $\{1, \dots, n-1\}$. On the other hand, any such $(r-1)$-subset defines a unique path from $(0, 0)$ to (r, n) which is a strictly ascending staircase. We can recover the corresponding partition $a \in \Pi_r(n)$ from this path uniquely. Thus, $|\Pi_r(n)| = \binom{n-1}{r-1}$.

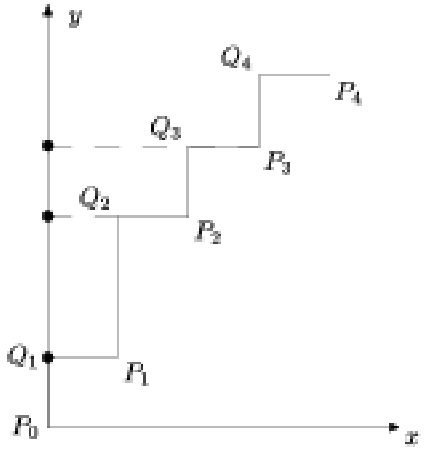


Figure 1.6: The Partition $(1, 2, 1, 1)$ as a Staircase

(vi) Any r-partition $a \in \Pi^*_r(n)$ with k nonzero parts can be turned into a k-partition $\hat{a} \in \Pi_k(n)$ by removing all zero parts. There are $\binom{r}{k}$ possibilities to obtain the same $\hat{a} \in \Pi_k(n)$ from different $a \in \Pi^*_r(n)$. This yields

$$\left|\Pi^*_r(n)\right| = \sum_{k=1}^{n} \binom{n}{k} \left|\Pi_k(n)\right| = \sum_{k=1}^{n} \binom{n}{k} \binom{n-1}{k-1}.$$

(vii) By definition, $\left|\overline{\Pi}_r(n)\right| = P_{n,r}$.

(viii) Removing the zero parts of an generalized unordered partition $a \in \overline{\Pi}^*_r(n)$ yields an element of $\overline{\Pi}_k(n)$ for some $k \leq r$. Thus, $\left|\overline{\Pi}^*_r(n)\right| = \sum_{k=1}^{r} P_{n,k}$.

$\square$

1.3.16 Theorem *(Multinomial Theorem) Let $m, n \in \mathbb{N}$. Then in $\mathbb{Z}[x_1, \ldots, x_m]$*

$$(x_1 + x_2 + \ldots + x_m)^n = \sum_{\substack{a_1 \geq 0, \ldots, a_m \geq 0 \\ \sum_{i=1}^{m} a_i = n}} \binom{n}{a_1, \ldots, a_m} x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$$

$$= \sum_{r=1}^{n} \sum_{\substack{a_1 \geq 1, \ldots, a_r \geq 1 \\ \sum_{i=1}^{r} a_i = n}} \binom{n}{a_1, \ldots, a_r} \sum_{\substack{S \in \binom{\{1, \ldots, m\}}{r} \\ S = \{s_1, \ldots, s_r\}}} \prod_{i=1}^{r} x_{s_i}^{a_i}.$$

In particular,

$$m^n = \sum_{a \in \Pi_m^*(n)} \binom{n}{a}.$$

Proof: (Cf. Halder and Heise [11, Satz (1.19)]) Each term in the product $(x_1 + x_2 + \ldots + x_m)^n$ is a word of length n in the indeterminates $x_1, \ldots, x_m$ and each such word appears exactly once (if the ordering of the "‘letters"’ x_i is preserved). As the indeterminates commute, we may rewrite every word in its standard form $x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$ with nonnegative a_i satisfying $\sum_{i=1}^{m} a_i = n$. Thus, $a = (a_1, \ldots, a_m) \in \Pi_m^*(n)$. By Lemma 1.3.6, for fixed a there are exactly $\binom{n}{a}$ ways to arrange the letters of this word in different ways. Each such rearragement occurs once when multiplying out the product on the left hand side. This proves the first formula. In the second formula, all nonzero parts of the partition are collected. The second sum allows to distribute the nonzero parts over all indeterminates $x_1, \ldots, x_m$. □

For $n \in \mathbb{N}$ we define the falling and raising factorials:

$$[x]_n := x \cdot (x-1) \cdots (x-n+1),$$
$$[x]^n := x \cdot (x+1) \cdots (x+n-1),$$

with $[x]_0 = [x]^0 = 1$. The three polynomial sequences

$$\{x^n \mid n \geq 0\}, \quad \{[x]_n \mid n \geq 0\}, \quad \{[x]^n \mid n \geq 0\}$$

form three bases for the space of polynomials over the rational numbers. Let us collect some properties of the Stirling and the Bell numbers:

1.3.17 Lemma *Let $n, k \in \mathbb{N}$. Then,*

(i) $\mathcal{S}_2(0,0) = 1$ *and* $\mathcal{S}_2(n,0) = \mathcal{S}_2(0,k) = 0$ *for* $n, k > 0$,

(ii) $\mathcal{S}_2(n+1,k) = \mathcal{S}_2(n,k-1) + k \cdot \mathcal{S}_2(n,k)$ *for* $n \geq 0$ *and* $k > 0$,

(iii) $\mathcal{S}_2(n+1,k) = \sum_{j=0}^{n} \binom{n}{j} \mathcal{S}_2(j,k-1)$ *for* $n \geq 0$ *and* $k > 0$.

(iv) $x^n = \sum_{k=0}^{n} \mathcal{S}_2(n,k)[x]_k$,

Proof:

(i) Follows from the definition of the Stirling numbers of the second kind.

(ii) Siehe Halder / Heise [11, Satz (4.3), Seite 57]

(iii) Siehe Halder / Heise [11, Satz (4.4), Seite 57]

(iv) Siehe Halder / Heise [11, Satz (4.1), Seite 56]

□

The *signless Stirling numbers of the first kind* for $n, k \in \mathbb{N}$ are

$$r(n,k) = |\{g \in \mathrm{Sym}_n \mid c(g) = k\}|,$$

where $c(g)$ is the number of cyclic factors of the element $g \in \mathrm{Sym}_n$, i. e. the number of orbits of $\langle g \rangle$ on the set $\{1, \ldots, n\}$.

1.3.18 Lemma

(i) For $n \geq 0$ *and* $k > 0$ *the recursion*

$$r(n+1,k) = r(n,k-1) + n \cdot r(n,k)$$

is satisfied. The initial values are

$$r(0,0) = 1 \quad \text{and} \quad r(n,0) = r(0,k) = 0 \quad \text{for} \quad n,k > 0.$$

(ii)

$$r(n,k) = \sum_{a \in \overline{\Pi}_k(n)} \frac{1}{k!} \binom{|\Delta a'|}{\Delta a'} \binom{n}{a} \prod_{i=1}^{k} (a_i - 1)!.$$

Proof:

(i) Kerber [13, page 82].

(ii) Let $N = \{1, \dots, n\}$ and let $a \in \overline{\Pi}_k(n)$ be a fixed cycle structure for an element in Sym_n with exactly k cycles. According to Lemma 1,3,10, the number of set partitions $\mathcal{P}$ of N with k unordered classes of size a_i f"ur $a \in \Pi_k(n)$ is $\frac{1}{k!}\binom{|\Delta a'|}{\Delta a'}\binom{n}{a}$. Within each class of $\mathcal{P}$ of size a_i, we can arrange the elements in $(a_i - 1)!$ ways to different cycles. This proves the stated number of elements in Sym_n with k cyclic factors.

□

The *Stirling numbers of the first kind* are

$$\mathcal{S}_1(n,k) := (-1)^{n+k} \cdot r(n,k).$$

1,3,19 Theorem

(i) The Stirling numbers of the first kind $\mathcal{S}_1(n,k)$ satisfy for $k > 0$ and $n \geq 0$ the recursion

$$\mathcal{S}_1(n+1,k) = \mathcal{S}_1(n,k-1) - n \cdot \mathcal{S}_1(n,k).$$

The initial values are

$$\mathcal{S}_1(0,0) = 1 \quad \textit{and} \quad \mathcal{S}_1(n,0) = \mathcal{S}_1(0,k) = 0 \quad \textit{for} \;\; n,k > 0.$$

(ii)

$$\mathcal{S}_1(n,k) = (-1)^{n+k} \sum_{a \in \overline{\Pi}_k(n)} \frac{1}{k!} \binom{|\Delta a'|}{\Delta a'} \binom{n}{a} \prod_{i=1}^{k} (a_i - 1)!.$$

(iii) *Let $n \in \mathbb{N}$. Then*

$$[x]_n = \sum_{k=0}^{n} \mathcal{S}_1(n,k) \cdot x^k.$$

(iv) *(Stirlings inversion formula)*

$$\sum_{i=0}^{n} \mathcal{S}_1(n,i) \cdot \mathcal{S}_2(i,k) = \sum_{i=k}^{n} \mathcal{S}_1(n,i) \cdot \mathcal{S}_2(i,k) = \delta_{n,k}.$$

Proof:

(i) Follows from Lemma 1.3.18 (i).

(ii) Follows from Lemma 1.3.18 (ii).

(iii) (Following Halder and Heise [11, Satz (5.3)]) For $n = 0$ the stated equation is trivially true. Thus let $n > 0$. We put $[x]_n = \sum_{k=0}^{n} s'(n,k)x^k$ with unknown coefficients $s'(n,k)$. Obviously, $s'(n,k) = 0 = \mathcal{S}_1(n,k)$ for $k > n$. If $n > 0$, the constant terms in $[x]_{n+1}$ and $[x]_n$ are zero, so $s'(n+1,0) = s'(n,0) = \mathcal{S}_1(n,0) = 0$. Thus

$$\begin{aligned}
\sum_{k=1}^{n+1} s'(n+1,k)x^k &= [x]_{n+1} \\
&= (x-n) \cdot [x]_n \\
&= \sum_{k=0}^{n} s'(n,k)x^{k+1} - \sum_{k=1}^{n} n \cdot s'(n,k)x^k \\
&= \sum_{k=1}^{n+1} s'(n,k-1)x^k - \sum_{k=1}^{n+1} n \cdot s'(n,k)x^k \\
&= \sum_{k=1}^{n+1} \big(s'(n,k-1) - n \cdot s'(n,k)\big)x^k.
\end{aligned}$$

Comparing coefficients on both sides we see that the $s'(n,k)$ fulfill the same recursion formula as the $\mathcal{S}_1(n,k)$. Equality of the initial values implies that $s'(n,k) = \mathcal{S}_1(n,k)$ for all $n, k \in \mathbb{N}$.

(iv) (Following Halder and Heise [11, Satz (5.4)]) By Lemma 1.3.17 (iv), $x^n = \sum_{k=0}^{n} \mathcal{S}_2(n,k)[x]_k$ for $n \in \mathbb{N}$. Together with (iii) this implies that the matrices $(\mathcal{S}_1(n,k))$ and $(\mathcal{S}_2(n,k))$ are mutually inverse. Together with the fact that both matrices are lower triangular, this yields the equations.

□

Table 1.2 shows the Stirling numbers of the first kind $\mathcal{S}_1(n,k)$ for small n and k.

	$\mathcal{S}_1(n,k), k =$									
n	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0
2	0	-1	1	0	0	0	0	0	0	0
3	0	2	-3	1	0	0	0	0	0	0
4	0	-6	11	-6	1	0	0	0	0	0
5	0	24	-50	35	-10	1	0	0	0	0
6	0	-120	274	-225	85	-15	1	0	0	0
7	0	720	-1764	1624	-735	175	-21	1	0	0
8	0	-5040	13068	-13132	6769	-1960	322	-28	1	0
9	0	40320	-109584	118124	-67284	22449	-4536	546	-36	1

Table 1.2: Stirling Numbers of the First Kind $\mathcal{S}_1(n,k)$

The following useful result can be found in Aigner [1]. We will need it later. We mention it here, even if it has nothing to do with partitions.

1,3,20 Lemma *Let* $\mathcal{B} = \left(b_{i,j}\right)$ *with* $b_{i,j} = \binom{j}{i}$ *for* $0 \leq i, j \leq n$ *be the matrix of binomial coefficients. The the inverse matrix* $\mathcal{B}^{-1} = (b'_{i,j})$ *has the coefficients* $b'_{i,j} = (-1)^{i+j}\binom{j}{i}$ *for* $0 \leq i, j \leq n$.

Chapter 2

Intersection Numbers of Designs

In this chapter we present the theory of intersection numbers of designs. Section 2.1 discussses ordinary intersection numbers, in particular results of Mendelsohn (Theorem 2.1.1) and Köhler (Theorem 2.1.2). The equations presented by Köhler in the latter theorem may be used to prove the nonexstence of designs for certain parameter cases.

In Section 2.2, higher intersection numbers are defined. We present results of Tran van Trung et al. [28] which generalize the results of the previous section for these more general kinds of numbers.

In Section 2.3, I present global intersection numbers of designs. These numbers are obtained by generalizing the higher intersection numbers. The main reason for introducing these numbers is that they are useful as invariants for designs and thus may help classifying designs with respect to isomorphism. For technical reasons, two different kinds of numbers are introduced. However, it turns out that there is a close relation between these two kinds of numbers which is given by the Stirling numbers of the first and second kind.

2.1 Ordinary Intersection Numbers

Already in 1971, intersection numbers of designs appear in Mendelsohn [22]. In this section, we present the two basic results of Mendelsohn and Köhler.

Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-design and $M \subseteq \mathcal{V}$ with $|M| = m$. Let

$$\alpha_i(M) = \Big| \big\{ B \in \mathcal{B} : \ \big| B \cap M \big| = i \ \big\} \Big|$$

be the number of blocks of the design intersecting M in exactly i points. We call $\alpha_i(M)$ the *i-th intersection number of M with $\mathcal{D}$*. The vector

$$\alpha(M) = \big(\alpha_0(M),\ \alpha_1(M),\ \ldots,\ \alpha_m(M)\big)$$

is the *intersection type* of M with $\mathcal{D}$. If M is a k-subset of $\mathcal{V}$, then $\alpha_k(M) = 1$ is equivalent to $M = B_0 \in \mathcal{B}$. In this case $\alpha_i(B_0)$ is the *i-th block intersection number of B_0* and $\alpha(B_0)$ is the *block intersection type of B_0*.

The following result of 1971 is due to Mendelsohn [22]. It describes an important relation of the intersection numbers of a subset M among themselves:

2.1.1 Theorem *(Mendelsohn [22]) Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design and let $M \subseteq \mathcal{V}$ with $|M| = m$. Then, for $i = 0, 1, \ldots, t$,*

$$\sum_{j=i}^{m} \binom{j}{i} \alpha_j(M) = \binom{m}{i} \lambda_i . \tag{2.1}$$

Proof: We count the tuples

$$(I, B) \in \binom{M}{i} \times \mathcal{B} : \ I \subseteq B \cap M$$

in two different ways: Choosing the set $I \in \binom{M}{i}$ and determining the number of blocks containing I we get the right hand side of (2.1). On the other hand, for $j = i, \ldots, m$ we may choose exactly $\alpha_j(M)$ blocks intersecting M in j points. Within these j-sets we can choose i-subsets I in $\binom{j}{i}$ different ways. This is the left hand side of (2.1). $\square$

The coefficient matrix of the equations on the left hand side of (2.1) has a special form: In its first $(t + 1)$ columns, the matrix is upper triangular with ones on the diagonal. These columns correspond to the intersection numbers $\alpha_0(M), \ldots, \alpha_t(M)$. To the right, this matrix is extended by some additional columns belonging to the intersection numbers $\alpha_{t+1}(M), \ldots, \alpha_m(M)$. We have the following result of Köhler [18].

2.1.2 Theorem *(Köhler [18]) Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design with $M \subseteq \mathcal{V}$ and $|M| = m \geq t$. Then, for $i = 0, 1, \ldots, t$:*

$$\alpha_i(M) = \sum_{h=i}^{t} (-1)^{h+i} \binom{h}{i} \binom{m}{h} \lambda_h$$
$$+ (-1)^{t+i+1} \sum_{h=0}^{m-t-1} \binom{t+h-i}{h} \binom{t+h+1}{i} \alpha_{t+h+1}(M). \quad (2.2)$$

Köhler proves this Theorem by induction. We omit this prove as we will later get a shorter proof from Theorem 2.2.4.

The equations of Köhler are useful for ruling out the existence of some designs. The following example can be found in Köhlers article:

2.1.3 Example The parameters 13-(32, 16, 3) are admissible. Assume there is a design $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ with these parameters. We may choose $M \subseteq \mathcal{V}$ with $m = |M| = 15$. Then by (2.2),

$$\alpha_1(M) = 105 - 14\alpha_{14}(M) - 195\alpha_{15}(M).$$

It is possible to choose M in such a way that at least one block of the design fully contains M. Thus $\alpha_{15}(M) \geq 1$. Then

$$\alpha_1(M) + 14\alpha_{14}(M) + 195\alpha_{15}(M) = 105,$$

which is impossible as $\alpha_1(M)$ and $\alpha_{14}(M)$ are nonnegative integers. Thus, a 13-(32, 16, 3) design does not exist. ◇

2.2 Intersection Numbers of Higher Order

Intersection numbers can be generalized as described in the article of Tran van Trung et al. [28].

In this section, we generalize the concept of intersection numbers of designs as seen in the previous section. Let again $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design with $\mathcal{B} = \{B_1, \ldots, B_b\}$ the set of blocks. For $M \subseteq \mathcal{V}$ and any integer $s \geq 1$ we put

$$\alpha_i^{(s)}(M) := \left| \left\{ \{B_{i_1}, \ldots, B_{i_s}\} \in \binom{\mathcal{B}}{s} : \left| \bigcap_{h=1}^{s} B_{i_h} \cap M \right| = i \right\} \right|,$$

i. e. the number of s-subsets of $\mathcal{B}$ intersecting M together in i points. We call this number the *i-th intersection number of order s of the set M with the design*. The vector

$$\alpha^{(s)}(M) := \left(\alpha_0^{(s)}(M), \ldots, \alpha_k^{(s)}(M) \right)$$

is the *intersection type of order s of M with the design $\mathcal{D}$*. We have $\alpha_i^{(1)}(M) = \alpha_i(M)$ for all i, i. e. the intersection numbers of higher order generalize the ordinary intersection numbers naturally.

In addition, we consider refinements of the parameters $\lambda_{i,j}$ of a t-design. Let I and J be disjoint subsets of $\mathcal{V}$ with $|I| = i$ and $|J| = j$ and $i + j \leq t$. Then for any integer $s \geq 1$ we put

$$\lambda_{i,j}^{(s)} = \left| \left\{ \{B_{i_1}, \ldots, B_{i_s}\} \in \binom{\mathcal{B}}{s} : I \subseteq \bigcap_{h=1}^{s} B_{i_h} \subseteq J^c \right\} \right|,$$

where $J^c := \mathcal{V} \setminus J$ is the complement of J in the set $\mathcal{V}$. Setting s equal to 1 gives

$\lambda_{i,j}^{(1)} = \lambda_{i,j}$. If $s = 1$ and $j = 0$ we write $\lambda_i = \lambda_{i,0}^{(1)}$. In particular, $\lambda = \lambda_{t,0}^{(1)}$.

2.2.1 Lemma *(Tran van Trung, Qiu-rong Wu, Dale M. Mesner [28]) Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. Let $I \in \binom{\mathcal{V}}{i}$ and $J \in \binom{\mathcal{V}}{j}$ be disjoint subsets of $\mathcal{V}$ of cardinalities i and j where $i + j \leq t$. Then for any integer $s \geq 1$:*

$$\lambda_{i,j}^{(s)} = \sum_{u=0}^{j} (-1)^u \binom{j}{u} \binom{\lambda_{i+u}}{s}.$$

In particular, the numbers $\lambda_{i,j}^{(s)}$ depends only on i and j but not on the choice of the subsets I and J with the required properties.

Proof: (following Tran van Trung et al. [28]) Call an s-subset of blocks $\{B_{i_1}, \ldots, B_{i_s}\} \in \binom{\mathcal{B}}{s}$ *admissible* if

$$I \subseteq \bigcap_{h=1}^{s} B_{i_h} \subseteq J^c$$

holds. In order to determine the requested number of admissible s-sets we distinguish two different types:

type i) There exists a block which is disjoint to J, i. e. there is an $h \leq s$ with $B_{i_h} \cap J = \emptyset$.

type ii) None of the blocks $B_{i_1}, \ldots, B_{i_h}$ is disjoint from J, i. e. $B_{i_h} \cap J \neq \emptyset$ for all $h = 1, \ldots, s$.

Let us first determine the number of admissible s-sets of blocks of type i). Let u be the number of blocks of the s-set which are disjoint from J. So,

$$u = |\{h \in \{1, \ldots, s\} \mid B_{i_h} \cap J = \emptyset\}| \geq 1.$$

Then there are $s - u$ blocks intersecting J non-trivially. We determine the number of possibilities to choose blocks $B \supseteq I$ with $B \cap J \neq \emptyset$. Put $R = B \cap J$. For any fixed $R \neq \emptyset$ with $|R| = r$ there are $\lambda_{i+r,j-r}$ blocks in the design containing I and intersecting J exactly in R. Thus, the overall number of blocks B with $I \subseteq B$ and $B \cap J \neq \emptyset$ equals

$$N = \sum_{\emptyset \neq R \subseteq J} \left|\{B \in \mathcal{B} \mid I \subseteq B,\ B \cap J = R\}\right| = \sum_{r=1}^{j} \binom{j}{r} \lambda_{i+r,j-r} = \lambda_i - \lambda_{i,j},$$

where the last equality follows from the fact that N is the number of blocks containing I which are not disjoint from J. Thus we determine the number of s-subsets of blocks of type i) to

$$\sum_{u=1}^{s} \binom{\lambda_{i,j}}{u} \binom{\lambda_i - \lambda_{i,j}}{s-u}.$$

We now determine the number of admissible s-sets of blocks of type ii). All the blocks of such an s-set contain I but no element of J is contained in all of them. We determine this number of s-sets of blocks using the principle of inclusion / exclusion (Lemma 1.2.3). Let Ω be the set of s-subsets of blocks which all contain I but none of which is totally disjoint from J. So, $|\Omega| = \binom{N}{s} = \binom{\lambda_i - \lambda_{i,j}}{s}$. For $y \in Y$ we put

$$A_y := \left\{ \{B_{i_1}, \ldots, B_{i_s}\} \in \Omega \;\middle|\; y \in \bigcap_{h=1}^{s} B_{i_h} \right\}.$$

For $Y \subseteq J$, $Y = \{y_1, \ldots, y_u\}$, let

$$A_Y = \bigcap_{h=1}^{u} A_{y_h}.$$

The requested number of s-sets of type ii) is the cardinality of

$$\hat{\Omega} = \Omega \setminus \bigcup_{y \in J} A_y,$$

which by inclusion / exclusion is equal to

$$|\hat{\Omega}| = |\Omega| + \sum_{u=1}^{j} (-1)^u \sum_{\substack{Y=\{y_1,\dots,y_u\}\subseteq J,\\ |Y|=u}} \left| \bigcap_{h=1}^{u} A_{y_h} \right|,$$

where $\bigcap_{h=1}^{u} A_{y_h}$ is a set of s-tuples of blocks which all contain I and u further points of J. The cardinality of this set is $\binom{\lambda_{i+u}}{s}$, and this number does not depend on the choice of the points $y_1, \dots, y_u$. So we get

$$|\hat{\Omega}| = \binom{\lambda_i - \lambda_{i,j}}{s} + \sum_{u=1}^{j} (-1)^u \cdot \binom{j}{u}\binom{\lambda_{i+u}}{s}.$$

Putting the results for the number of admissible s-subsets of type i) and ii) together, we obtain

$$\begin{aligned}
\lambda_{i,j}^{(s)} &= \sum_{u=1}^{s} \binom{\lambda_{i,j}}{u}\binom{\lambda_i - \lambda_{i,j}}{s-u} + \binom{\lambda_i - \lambda_{i,j}}{s} + \sum_{u=1}^{j} (-1)^u \binom{j}{u}\binom{\lambda_{i+u}}{s} \\
&= \sum_{u=0}^{s} \binom{\lambda_{i,j}}{u}\binom{\lambda_i - \lambda_{i,j}}{s-u} + \sum_{u=1}^{j} (-1)^u \binom{j}{u}\binom{\lambda_{i+u}}{s}.
\end{aligned}$$

Using the following formula for binomial coefficients from [12, page 1429]

$$\sum_{i=0}^{n} \binom{n}{i}\binom{m}{r-i} = \binom{n+m}{r}$$

we get the stated result:

$$\begin{aligned}
\lambda_{i,j}^{(s)} &= \binom{\lambda_i}{s} + \sum_{u=1}^{j} (-1)^u \binom{j}{u}\binom{\lambda_{i+u}}{s} \\
&= \sum_{u=0}^{j} (-1)^u \binom{j}{u}\binom{\lambda_{i+u}}{s}.
\end{aligned}$$

□

The next steps will be devoted to generalizing the theorems of Mendelsohn (Theorem 2,1,1) and Köhler (Theorem 2,1,2) for intersection numbers of higher order. Let us make some definitions first, then we come back to this lemma.

Let $\mathcal{A} = (a_{i,j})$ be a 0/1-matrix with u rows and v columns. We label the rows and columns by natural numbers using the index sets $\mathcal{R} = \{1, 2, \ldots, u\}$ and $\mathcal{C} = \{1, 2, \ldots, v\}$.

(i) Let $J = \{j_1, j_2, \ldots, j_n\} \subseteq \mathcal{C}$. Then let

$$J' = \{i \in \mathcal{R} \mid a_{i,j_1} = a_{i,j_2} = \ldots = a_{i,j_n} = 1\} \subseteq \mathcal{R}$$

be the set of indices of rows, which have an entry one everywhere in the columns indexed by elements of J.

(ii) Let $I = \{i_1, i_2, \ldots, i_m\} \subseteq \mathcal{R}$. Then let

$$I' = \{j \in \mathcal{C} \mid a_{i_1,j} = a_{i_2,j} = \ldots = a_{i_m,j} = 1\} \subseteq \mathcal{C}$$

be the set of indices of columns, which have an entry one everywhere in the rows indexed by elements of I.

2,2,2 Lemma *(Tran van Trung, Qiu-rong Wu, Dale M. Mesner [28])Let $\mathcal{A}$ be a 0/1-matrix with u rows and v columns, indexed by sets $\mathcal{R} = \{1, 2, \ldots, u\}$ and $\mathcal{C} = \{1, 2, \ldots, v\}$. Then, for all $m, n \in \mathbb{N}$:*

$$\sum_{I \in \binom{\mathcal{Z}}{m}} \binom{|I'|}{n} = \sum_{J \in \binom{\mathcal{S}}{n}} \binom{|J'|}{m}.$$

Proof: If one if the numbers m and n is zero or if $m > u$ or $n > v$ then the equation is trivially true. We may thus require $1 \leq m \leq u$ and $1 \leq n \leq v$. For $I \subseteq \mathcal{R}$ and $J \subseteq \mathcal{C}$ let $\mathcal{A}_{[I],[J]}$ be the $(|I| \times |J|)$-submatrix of $\mathcal{A}$, formed by the elements lying in the intersection of rows indexed by elements of I and columns indexed by elements of J. Then, with $\underline{1}_{m,n}$ the $(m \times n)$-matrix whose entries are all one,

$$\left| \left\{ I \in \binom{\mathcal{R}}{m},\ J \in \binom{\mathcal{C}}{n} \;\middle|\; \mathcal{A}_{[I],[J]} = \underline{1}_{m,n} \right\} \right| = \sum_{I \in \binom{\mathcal{R}}{m}} \binom{|I'|}{n} = \sum_{J \in \binom{\mathcal{C}}{n}} \binom{|J'|}{m}.$$

□

The next theorem generalizes the equations of Mendelsohn (2.1) to intersection numbers of higher order:

2.2.3 Theorem *(Tran van Trung, Qiu-rong Wu, Dale M. Mesner [28]) Let* $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ *be a* t-(v, k, λ) *design. Let* $M \subseteq \mathcal{V}$ *with* $|M| = m$*. Then, for any natural number* $s \geq 1$ *and for all* i *with* $0 \leq i \leq t$*:*

$$\sum_{j=i}^{m} \binom{j}{i} \alpha_j^{(s)}(M) = \binom{m}{i}\binom{\lambda_i}{s}. \tag{2.3}$$

Proof: Let $\mathcal{N} = (n_{i,j})$ be the incidence matrix of the design. As in Lemma 2.2.2, let $\mathcal{C} = \{1, 2, \ldots, b\}$ be the index set for the columns of $\mathcal{N}$. We consider $\mathcal{N}_{[M],[\mathcal{C}]}$, the $(m \times b)$-submatrix of $\mathcal{N}$ which consists of the rows of $\mathcal{N}$ belonging to the elements of M. For any i-subset $I = \{x_1, \ldots, x_i\} \subseteq M$, let I' be the set of column indices of blocks containing I, i. e.

$$I' = \{j \mid 0 \leq j \leq b : \ n_{x_h, j} = 1 \text{ for } \ h = 1, \ldots, i\}.$$

In the same vain, for any set $J = \{y_1, \ldots, y_j\} \subseteq \mathcal{C}$ let

$$J' = \{x \in M \mid n_{x, y_h} = 1 \text{ for } \ h = 1, \ldots, j\}.$$

For any $I \in \binom{M}{i}$, there are $|I'| = \lambda_i$ blocks incident with I. From this set of blocks, we get $\binom{|I'|}{s}$ s-sets of blocks containing I in their intersection. As we have $\binom{m}{i}$ possibilities for $I \subseteq M$, we get

$$\binom{m}{i}\binom{\lambda_i}{s} = \sum_{I \in \binom{M}{i}} \binom{I'}{s}$$

which by Lemma 2.2.2 is equal to

$$= \sum_{J \in \binom{\mathcal{B}}{s}} \binom{J'}{i}$$

and by counting the set $(I, \{B_{i_1}, \ldots, B_{i_s}\}) \in \binom{M}{i} \times \binom{\mathcal{B}}{s} : \; I \subseteq M \cap \bigcap_{h=1}^{s} B_{i_h}$ in two different ways we get

$$= \sum_{j=i}^{m} \binom{j}{i} \alpha_j^{(s)}(M).$$

□

The following theorem generalizes Theorem 2.1.2. The proof is a generalization of Bolick's proof of the Theorem of Köhler [7].

2.2.4 Theorem *(Tran van Trung, Qiu-rong Wu, Dale M. Mesner [28]) Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design and let $M \subseteq \mathcal{V}$ with $|M| = m \geq t$. Then, for any integer $s \geq 1$ and for all $i = 0, 1, \ldots, t$:*

$$\alpha_i^{(s)}(M) = \sum_{h=i}^{t} (-1)^{h+i} \binom{h}{i} \binom{m}{h} \binom{\lambda_h}{s} + (-1)^{t+i+1} \sum_{h=0}^{m-t-1} \binom{t+h-i}{h} \binom{t+h+1}{i} \alpha_{t+h+1}^{(s)}(M). \tag{2.4}$$

Proof: Let $\alpha^{(s)}(M) = \left(\alpha_0^{(s)}(M), \ldots, \alpha_m^{(s)}(M)\right)$ be the intersection type of M and let $\mathfrak{y} = (y_0, \ldots, y_t)$ be the vector with entries $y_i = \binom{m}{i}\binom{\lambda_i}{s}$ for $0 \leq i \leq t$. Rewriting equation (2.1) in terms of matrices and vectors we get

$$\mathscr{B}_{[0..t],[0..k]} \cdot \alpha^{(s)}(M)^{\top} = \mathfrak{y}^{\top}.$$

Splitting the vector $\alpha^{(s)}(M)$ into two parts, and indicating the set of selected indices in the index, we get

$$\alpha^{(s)}_{[0,\dots,t]}(M) = \big(\alpha^{(s)}_0(M), \dots , \alpha^{(s)}_t(M)\big),$$

holding the first $(t+1)$ elements and

$$\alpha^{(s)}_{[t+1,\dots,k]}(M) = \big(\alpha^{(s)}_{t+1}(M), \dots , \alpha^{(s)}_k(M)\big),$$

containing the remaining coefficients. Then (2.1) yields

$$\begin{aligned}
&\mathcal{B}_{[0,\dots,t],[0,\dots,t]} \cdot \alpha^{(s)}_{[0,\dots,t]}(M)^\top = -\mathcal{B}_{[0,\dots,t],[t+1,\dots,k]} \cdot \alpha^{(s)}_{[t+1,\dots,k]}(M)^\top + \mathfrak{y}^\top \\
&\iff \alpha^{(s)}_{[0,\dots,t]}(M)^\top = -\mathcal{B}^{-1}_{[0,\dots,t],[0,\dots,t]} \cdot \mathcal{B}_{[0,\dots,t],[t+1,\dots,k]} \cdot \alpha^{(s)}_{[t+1,\dots,k]}(M)^\top \\
&\qquad\qquad + \mathcal{B}^{-1}_{[0,\dots,t],[0,\dots,t]} \cdot \mathfrak{y}^\top,
\end{aligned}$$

where $\mathcal{B}^{-1} = (b'_{i,j})$ is the inverse of the matrix $\mathcal{B}$. By Lemma 1.3.20, this matrix has the coefficients $b'_{i,j} = (-1)^{i+j}\binom{j}{i}$. In the i-th row we get for $0 \le i \le t$:

$$\alpha^{(s)}_i(M) = -\sum_{h=t+1}^{m} \underbrace{\sum_{j=i}^{t}(-1)^{i+j}\binom{j}{i}\binom{h}{j}}_{=:C_h}\alpha^{(s)}_h(M) + \sum_{h=i}^{t}(-1)^{i+h}\binom{h}{i}\binom{m}{h}\binom{\lambda_h}{s}.$$

We consider C_h more closely, using the following equation of Knuth [17]

$$\sum_{j=0}^{m}(-1)^j\binom{n}{j} = (-1)^m\binom{n-1}{m}. \tag{2.5}$$

We obtain

$$\begin{aligned}
C_h &= \sum_{j=i}^{t}(-1)^{i+j}\binom{j}{i}\binom{h}{j} \\
&= \sum_{j=0}^{t-i}(-1)^j\binom{j+i}{i}\binom{h}{j+i}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=0}^{t-i} (-1)^j \frac{(j+i)!}{i!\,j!} \frac{h!}{(j+i)!\,(h-j-i)!} \\
&= \left[\sum_{j=0}^{t-i} (-1)^j \frac{(h-i)!}{j!\,(h-j-i)!} \right] \binom{h}{i} \\
&= \left[\sum_{j=0}^{t-i} (-1)^j \binom{h-i}{j} \right] \binom{h}{i} \\
&\overset{(2.5)}{=} (-1)^{t-i} \binom{h-i-1}{t-i} \binom{h}{i} \\
&= (-1)^{t-i} \binom{h-i-1}{h-t-1} \binom{h}{i}.
\end{aligned}
$$

Inserting this expression for C_h, we get the stated equation after a shift of the index:

$$
\begin{aligned}
&\alpha_i^{(s)}(M) \\
&= -\sum_{h=t+1}^{m} (-1)^{t-i} \binom{h-i-1}{h-t-1} \binom{h}{i} \alpha_h^{(s)}(M) + \sum_{h=i}^{t} (-1)^{i+h} \binom{h}{i} \binom{m}{h} \binom{\lambda_h}{s} \\
&= (-1)^{t+i+1} \sum_{h=0}^{m-t-1} \binom{t+h-i}{h} \binom{t+h+1}{i} \alpha_{t+h+1}^{(s)}(M) \\
&\qquad + \sum_{h=i}^{t} (-1)^{i+h} \binom{h}{i} \binom{m}{h} \binom{\lambda_h}{s}.
\end{aligned}
$$

□

Choosing $s = 1$, this yields a proof of Theorem 2.1.2

2.3 Global Intersection Numbers

In order to obtain invariants of the design we define global intersection numbers. We extend the theory presented in the previous sections to the new kind of numbers:

Let again $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design. For any integer $s > 1$ and any $i \in \mathbb{N}$ we put

$$\alpha_i^{(s)}(\mathcal{D}) = \left| \left\{ \{B_{j_1}, \ldots, B_{j_s}\} \in \binom{\mathcal{B}}{s} : \left| \bigcap_{h=1}^{s} B_{j_h} \right| = i \right\} \right|,$$

i. e. the number of s-subsets of blocks of the design intersecting in exactly i points. We call this the *i-th global intersection number of order s of the design $\mathcal{D}$*. Obviously, $\alpha_i^{(s)}(\mathcal{D}) = 0$ for $i > k$ and $\alpha_k^{(s)}(\mathcal{D})$ is 0 for $s > 1$ and b otherwise. The vector

$$\alpha^{(s)}(\mathcal{D}) = \left(\alpha_0^{(s)}(\mathcal{D}), \ldots, \alpha_k^{(s)}(\mathcal{D})\right)$$

is the *global intersection type of order s of $\mathcal{D}$*.

We are interested in quickly determining the global intersection numbers of a design. We will present an algorithm to compute these numbers later in Section 5.1). The computation of a slightly different kind of numbers turns out to be simpler.

For $s \geq 1$ and $i \in \mathbb{N}$, we put

$$\alpha_i^{[s]}(\mathcal{D}) = \left| \left\{ (B_{j_1}, \ldots, B_{j_s}) \in \mathcal{B}^s : \left| \bigcap_{h=1}^{s} B_{j_h} \right| = i \right\} \right|,$$

i. e. the number of s-tuples of blocks intersecting in exactly i elements. We call this the *i-th global intersection number of s-tuples of blocks of the design*. We have $\alpha_i^{[s]}(\mathcal{D}) = 0$ for $i > k$. The vector

$$\alpha^{[s]}(\mathcal{D}) = \left(\alpha_0^{[s]}(\mathcal{D}), \ldots, \alpha_k^{[s]}(\mathcal{D})\right)$$

is the *global intersection type of s-tuples of blocks of $\mathcal{D}$*.

The connection between the $\alpha^{(s)}(\mathcal{D})$ and the $\alpha^{[s]}(\mathcal{D})$ is given by the Stirling numbers:

2.3.1 Theorem *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v, k, λ) design and let $0 < s \in \mathbb{N}$. Then:*

$$\alpha^{[s]}(\mathcal{D}) = \sum_{u=1}^{s} u!\, \mathfrak{s}_2(s, u)\, \alpha^{(u)}(\mathcal{D})$$

and

$$\alpha^{(s)}(\mathcal{D}) = \frac{1}{s!} \sum_{u=1}^{s} \mathfrak{s}_1(s, u)\, \alpha^{[u]}(\mathcal{D}).$$

Proof: We consider the power set $\mathfrak{P}(\mathcal{V})$ which forms a semigroup with respect to the composition $\cap$. As $M \cap M = M$ for all $M \subseteq \mathcal{V}$, all elements are idempotent. Let $(\mathbb{Z}[\mathfrak{P}(\mathcal{V})], \cap)$ be the *semigroup ring* over $\mathfrak{P}(\mathcal{V})$ with integral coefficients. The elements of this ring are of the form

$$a = \sum_{M \in \mathfrak{P}(\mathcal{V})} a_M \cdot M.$$

The multiplication within this ring is defined by the intersection of the elements of $\mathfrak{P}(\mathcal{V})$. Thus we write the symbol $\cap$ for the multiplication The sum and the intersection of two elements $a = \sum_{M \in \mathfrak{P}(\mathcal{V})} a_M \cdot M$ und $b = \sum_{M \in \mathfrak{P}(\mathcal{V})} b_M \cdot M$ in $\mathbb{Z}[\mathfrak{P}(\mathcal{V})]$ are

$$\begin{aligned} a + b &:= \sum_{M \in \mathfrak{P}(\mathcal{V})} (a_M + b_M) \cdot M, \\ a \cap b &:= \sum_{W \in \mathfrak{P}(\mathcal{V})} \sum_{\substack{M,N \in \mathfrak{P}(\mathcal{V}) \\ M \cap N = W}} (a_M \cdot b_N) \cdot W. \end{aligned}$$

We consider $\mathbb{Z}[\mathfrak{P}(\mathcal{V})]$ as a $\mathbb{Z}$-module. Another $\mathbb{Z}$-module is the space of integral row vectors $\mathcal{W}_v := \mathbb{Z}^{v+1} = \langle \mathfrak{e}_0, \ldots, \mathfrak{e}_v \rangle_{\mathbb{Z}}$. We define the following mapping, which we call the *weight map*

$$\kappa : \mathbb{Z}[\mathfrak{P}(\mathcal{V})] \to \mathbb{Z}^{v+1}, \quad \sum_{M \in \mathfrak{P}(\mathcal{V})} a_M \cdot M \mapsto \sum_{M \in \mathfrak{P}(\mathcal{V})} a_M \cdot \mathfrak{e}_{|M|}.$$

This map is a $\mathbb{Z}$-module homomorphism. The space $\mathcal{W}_v$ is called *weight space*. The mapping κ is useful for computing intersection numbers: Let $B_1, \ldots, B_b$ be the set of blocks of a design $\mathcal{D} = (\mathcal{V}, \mathcal{B})$. Then, for any integer $s \geq 1$:

$$\alpha^{[s]}(\mathcal{D}) = \kappa \left(\sum_{(B_{j_1}, \ldots, B_{j_s}) \in \mathcal{B}^s} \bigcap_{h=1}^{s} B_{j_h} \right) \tag{2.6}$$

and

$$\alpha^{(s)}(\mathcal{D}) = \kappa \left(\sum_{\substack{X \in \binom{\{1, \ldots, b\}}{s}, \\ X = \{x_1, \ldots, x_s\}}} \bigcap_{j=1}^{s} B_{x_j} \right). \tag{2.7}$$

By the Multinomial Theorem 1.3.16 we get

$$\begin{aligned}
\alpha^{[s]}(\mathcal{D}) &\overset{(2.6)}{=} \kappa \left(\sum_{(B_{j_1}, \ldots, B_{j_s}) \in \mathcal{B}^s} \bigcap_{h=1}^{s} B_{j_h} \right) \\
&= \kappa \left(\bigcap^{s} \sum_{j=1}^{b} B_j \right) \\
&\overset{1.3.16}{=} \kappa \left(\sum_{\substack{a_1 \geq 0, \ldots, a_b \geq 0 \\ \sum_{h=1}^{b} a_h = s}} \binom{s}{a_1, \ldots, a_b} \bigcap_{j=1}^{b} \bigcap^{a_j} B_j \right) = (*),
\end{aligned}$$

using the convention that $\bigcap^{0} S = \mathcal{V}$ for any set S. Now in the sum over all nonnegative $a_1, \ldots, a_b$ with $\sum_{h=1}^{b} a_h = s$, a lot of the a_h may be zero. Let $c_1, \ldots, c_u$ be the non-zero terms of this sequence with $\sum_{h=1}^{u} c_h = s$. We may thus split the sum by firstly choosing the set of positions $\{x_1, \ldots, x_u\}$ where the a_h are nonzero. This gives

$$(*) = \kappa \left(\sum_{u=1}^{s} \sum_{\substack{X \in \binom{\{1, \ldots, b\}}{u}, \\ X = \{x_1, \ldots, x_u\}}} \sum_{\substack{c_1 \geq 1, \ldots, c_u \geq 1, \\ \sum_{h=1}^{u} c_h = s}} \binom{s}{c_1, \ldots, c_u} \bigcap_{j=1}^{u} \underbrace{\bigcap^{c_j} B_{x_j}}_{= B_{x_j}} \right) = (**).$$

where we can exchange the two inner sums. In the rightmost intersection, we can neglect the exponent c_j as long as it is greater than zero (by idempotency, $\underbrace{M \cap M \cap \ldots \cap M}_{\geq 1 \text{ times}} = M$). We continue with

$$(**) = \kappa \left(\sum_{u=1}^{s} \sum_{\substack{c_1 \geq 1, \ldots, c_u \geq 1 \\ \sum_{k=1}^{u} c_k = s}} \binom{s}{c_1, \ldots, c_u} \sum_{\substack{X \in \binom{\{1,\ldots,b\}}{u}, \\ X = \{x_1, \ldots, x_u\}}} \bigcap_{j=1}^{u} B_{x_j} \right) = (***).$$

Now the inner sum is independent of the partition $c = (c_1, \ldots, c_u)$. We thus can take out the sum over all partitions as a scalar factor. Note that by Lemma 1.3.14, this factor is equal to $u! \cdot \mathfrak{S}_2(s, u)$. Using the $\mathbb{Z}$-linearity of κ and (2.7), we arrive at

$$\begin{aligned}
(***) &= \kappa \left(\sum_{u=1}^{s} \underbrace{\left(\sum_{\substack{c_1 \geq 1, \ldots, c_u \geq 1 \\ \sum_{k=1}^{u} c_k = s}} \binom{s}{c_1, \ldots, c_u} \right)}_{u! \cdot \mathfrak{S}_2(s,u)} \sum_{\substack{X \in \binom{\{1,\ldots,b\}}{u}, \\ X = \{x_1, \ldots, x_u\}}} \bigcap_{j=1}^{u} B_{x_j} \right) \\
&= \sum_{u=1}^{s} u! \cdot \mathfrak{S}_2(s, u) \cdot \kappa \left(\sum_{\substack{X \in \binom{\{1,\ldots,b\}}{u}, \\ X = \{x_1, \ldots, x_u\}}} \bigcap_{j=1}^{u} B_{x_j} \right) \\
&\overset{(2.7)}{=} \sum_{u=1}^{s} u! \cdot \mathfrak{S}_2(s, u) \cdot \alpha^{(u)}(\mathcal{D}),
\end{aligned}$$

which is the first stated equality. The second equality follows by combinatorial inversion using Theorem 1.3.19 (iii). Both equations are equivalent. $\square$

2.3.2 Lemma *Let $\mathcal{D}$ be a t-(v, k, λ) design. Then for any integer $s \geq 1$ and any integer i with $0 \leq i \leq t$,*

$$\sum_{j=i}^{k} \binom{j}{i} \alpha_j^{(s)}(\mathcal{D}) = \binom{v}{i} \binom{\lambda_i}{s},$$

and

$$\alpha_i^{(s)}(\mathcal{D}) = \sum_{h=i}^{t}(-1)^{h+i}\binom{h}{i}\binom{v}{h}\binom{\lambda_h}{s} + (-1)^{t+i+1}\sum_{h=0}^{k-t-1}\binom{t+h-i}{h}\binom{t+h+1}{i}\alpha_{t+h+1}^{(s)}(\mathcal{D}).$$

Proof: Putting $M := \mathcal{V}$ we get

$$\alpha_i^{(s)}(\mathcal{V}) = \alpha_i^{(s)}(\mathcal{D})$$

for $s \geq 1$ and $i \in \mathbb{N}$. The stated equalities then follow by Theorem 2.2.3 and by Theorem 2,2,4 with $m = v$. □

Chapter 3

The Construction of Designs

In this chapter we construct designs with a prescribed automorphism group. In Section 3.1, we present the method of Kramer and Mesner and discuss some small examples. The program package DISCRETA [3] developed by the author and colleagues from the University of Bayreuth around Prof. Dr. R. Laue may be used to construct designs in this manner. In Section 3.2, 8-(31, 10, λ) designs invariant under PSL(3, 5) are presented. Section 3.3 is merely a list of t-designs with large t (i. e. $t \geq 7$) which have been found by applying this method.

3.1 The Method of Kramer and Mesner

t-Designs with large t are difficult to construct. The following theorem of Kramer and Mesner [19] is a useful tool to construct designs with a prescribed automorphism group. This problem is transformed into the problem of finding the solutions of a system of diophantine equations. Thus, choosing a non-trivial group A simplifies the problem quite a bit. However, only designs which are invariant under this group can be found.

3.1.1 Theorem *(Earl S. Kramer, Dale M. Mesner [19]) Let t-(v, k, λ) be a putative design parameter set (we may require it to be an admissible parameter set,* *for instance). Let $\mathcal{V} = \{1, \ldots, v\}$ be a v-element set and let $A \leq \mathrm{Sym}_{\mathcal{V}}$ be a permutation group. Let $\mathfrak{D}^A_{t-(v,k,\lambda)}$ be the set of t-(v, k, λ) designs on $\mathcal{V}$ invariant under A. Assume A has ℓ_t orbits on t-subsets of $\mathcal{V}$ and ℓ_k orbits on k-subsets. Let $\mathcal{O}_{t,1}, \ldots, \mathcal{O}_{t,\ell_t}$ and $\mathcal{O}_{k,1}, \ldots, \mathcal{O}_{k,\ell_k}$ be the set of A-orbits on $\binom{\mathcal{V}}{t}$ and $\binom{\mathcal{V}}{k}$, respectively. Let $O_{i,j} \in \mathcal{O}_{i,j}$ be representing sets of these orbits for $i \in \{t, k\}$ and $1 \leq j \leq \ell_i$. For $i \leq \ell_t$ and $j \leq \ell_k$, put*

$$m_{i,j} = \left|\{K \in \mathcal{O}_{k,j} \mid O_{t,i} \subseteq K\}\right|.$$

We form the matrix

$$\mathcal{M}^A_{t,k} := (m_{i,j}).$$

Let $\mathfrak{L}^A_{t-(v,k,\lambda)}$ be the set of solutions of

$$\mathcal{M}^A_{t,k} \cdot \mathfrak{x}^\top = \lambda \cdot \underline{1}_{\ell_t \times 1} \tag{3.1}$$

with $\mathfrak{x} \in \{0, 1\}^{\ell_k}$. Then, the mappings

$$\mathfrak{D}^A_{t-(v,k,\lambda)} \to \mathfrak{L}^A_{t-(v,k,\lambda)}, \ \mathcal{D} = (\mathcal{V}, \mathcal{B}) \mapsto \mathfrak{x}_{\mathcal{B}}$$

with

$$\mathfrak{x}_{\mathcal{B}}(j) = 1 \iff \mathcal{O}_{k,j} \subseteq \mathcal{B}, \ \text{and} \ 0 \text{ otherwise}$$

and

$$\mathfrak{L}^A_{t-(v,k,\lambda)} \to \mathfrak{D}^A_{t-(v,k,\lambda)}, \quad \mathfrak{x} \mapsto \mathcal{D}_{\mathfrak{x}} = (\mathcal{V}, \mathcal{B}_{\mathfrak{x}})$$

with

$$\mathcal{B}_{\mathfrak{x}} = \bigcup_{\substack{j=1 \\ \mathfrak{x}(j)=1}}^{\ell_k} \mathcal{O}_{k,j}$$

are mutually inverse bijections between $\mathfrak{D}^A_{t-(v,k,\lambda)}$ and $\mathfrak{L}^A_{t-(v,k,\lambda)}$.

Proof: We first have to prove that the numbers $m_{i,j}$ are in fact well defined, i. e. independent of the choice of the representing set $O_{t,i} \in \mathcal{O}_{t,i}$. In order to stress the representing set, let us call the number in question

$$m_{i,j}(O) = |\{K \in \mathcal{O}_{k,j} \mid O \subseteq K\}|,$$

where the argument indicates which set $O \in \mathcal{O}_{t,i}$ has been used in the definition. Now, for any $a \in A$,

$$\begin{aligned} m_{i,j}(O_{t,i}^a) &= |\{K \in \mathcal{O}_{k,j} \mid O_{t,i}^a \subseteq K\}| \\ &= |\{K \in \mathcal{O}_{k,j} \mid O_{t,i} \subseteq K^{a^{-1}}\}| \\ &= |\{K \in \mathcal{O}_{k,j} \mid O_{t,i} \subseteq K\}| \\ &= m_{i,j}(O_{t,i}), \end{aligned}$$

where we used the fact that $\mathcal{O}_{k,j} = \mathcal{O}_{k,j}^a$ as it is an orbit under the group A. This shows that the numbers of the theorem are in fact well defined.

We now prove that for $\mathcal{D} = (\mathcal{V}, \mathcal{B}) \in \mathfrak{D}_{t-(v,k,\lambda)}^A$ the mapping $\mathcal{B} \mapsto \mathfrak{x}_{\mathcal{B}}$ with $\mathfrak{x}_{\mathcal{B}}(j) = 1 \Leftrightarrow O_{k,j} \in \mathcal{B} \Leftrightarrow \mathcal{O}_{k,j} \subseteq \mathcal{B}$ is well defined with image contained in $\mathfrak{L}_{t-(v,k,\lambda)}^A$. First, we note that as $A \leq \mathrm{Aut}(\mathcal{D})$, $O_{k,j} \in \mathcal{B}$ implies $O_{k,j}^a \in \mathcal{B}$ for all $a \in A$. Thus, $\mathcal{O}_{k,j}$ either is fully contained in $\mathcal{B}$ or $\mathcal{B} \cap \mathcal{O}_{k,j}$ is empty. This means that $\mathcal{B}$ is a union of whole orbits of A on k-subsets. The vector $\mathfrak{x}_{\mathcal{B}}$ simply records which k-orbits are contained in the design:

$$\mathfrak{x}_{\mathcal{B}}(j) = 1 \iff \mathcal{O}_{k,j} \subseteq \mathcal{B} \iff O_{k,j} \in \mathcal{B}.$$

We now show that the vector $\mathfrak{x}_{\mathcal{B}}$ lies in $\mathfrak{L}_{t-(v,k,\lambda)}^A$ by showing that it is a solution of (3.1). Let i be a number less than or equal to ℓ_t. Then,

$$\begin{aligned} \sum_{j=1}^{\ell_k} m_{i,j} \cdot \mathfrak{x}_{\mathcal{B}}(j) &= \sum_{\substack{j=1 \\ \mathcal{O}_{k,j} \subseteq \mathcal{B}}}^{\ell_k} |\{K \in \mathcal{O}_{k,j} \mid O_{t,i} \subseteq K\}| \\ &= |\{K \in \mathcal{B} \mid O_{t,i} \subseteq K\}| \end{aligned}$$

$$= \lambda.$$

Thus, $\mathcal{M}^A_{t,k} \cdot \mathfrak{x}^\top_{\mathcal{B}} = \lambda \cdot \underline{1}_{\ell_t \times 1}$ which implies $\mathfrak{x}_{\mathcal{B}} \in \mathfrak{L}^A_{t-(v,k,\lambda)}$.

On the other hand, let $\mathfrak{x} \in \mathfrak{L}^A_{t-(v,k,\lambda)}$ be a 0/1-vector of length ℓ_k with $\mathcal{M}^A_{t,k} \cdot \mathfrak{x}^\top = \lambda \cdot \underline{1}_{\ell_t \times 1}$. We must show that the block set $\mathcal{B}_{\mathfrak{x}}$ defines a t-(v, k, λ) design $\mathcal{D}_{\mathfrak{x}} = (\mathcal{V}, \mathcal{B}_{\mathfrak{x}})$ with $A \leq \mathrm{Aut}(\mathcal{D}_{\mathfrak{x}})$. Let T be an arbitrary t-subset of $\mathcal{V}$. Then there is an index $i \leq \ell_t$ and an element $a \in A$ with $T \in \mathcal{O}_{t,i}$ and $T^a = O_{t,i}$. Then

$$\begin{aligned}
\lambda &= \sum_{j=1}^{\ell_k} m_{i,j} \cdot \mathfrak{x}(j) \\
&= \sum_{\substack{j=1 \\ \mathfrak{x}(j)=1}}^{\ell_k} |\{K \in \mathcal{O}_{k,j} \mid O_{t,i} \subseteq K\}| \\
&= \sum_{\substack{j=1 \\ \mathfrak{x}(j)=1}}^{\ell_k} |\{K \in \mathcal{O}_{k,j} \mid O_{t,i}^{a^{-1}} \subseteq K^{a^{-1}}\}| \\
&= \sum_{\substack{j=1 \\ \mathfrak{x}(j)=1}}^{\ell_k} |\{K \in \mathcal{O}_{k,j}^{a^{-1}} = \mathcal{O}_{k,j} \mid T \subseteq K\}| \\
&= \left| \left\{ K \in \bigcup_{\substack{j=1 \\ \mathfrak{x}(j)=1}}^{\ell_k} \mathcal{O}_{k,j} \mid T \subseteq K \right\} \right| \\
&= |\{K \in \mathcal{B}_{\mathfrak{x}} \mid T \subseteq K\}|,
\end{aligned}$$

which implies that $\mathcal{B}_{\mathfrak{x}}$ is the block set of a t-(v, k, λ) design. Being a union of whole orbits under A, the block set $\mathcal{B}_{\mathfrak{x}}$ is invariant under this group. Thus $A \leq \mathrm{Aut}(\mathcal{D}_{\mathfrak{x}})$ and $\mathcal{D}_{\mathfrak{x}} \in \mathfrak{D}^A_{t-(v,k,\lambda)}$.

In addition, one easily verifies the equations

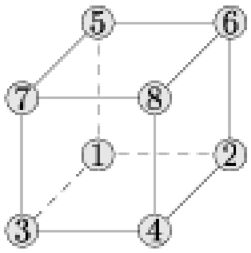
$$\mathcal{B}_{\mathfrak{x}_{\mathcal{B}}} = \mathcal{B} \quad \text{and} \quad \mathfrak{x}_{\mathcal{B}_{\mathfrak{x}}} = \mathfrak{x}.$$

This implies that the stated mappings between the sets $\mathfrak{L}^A_{t-(v,k,\lambda)}$ and $\mathfrak{D}^A_{t-(v,k,\lambda)}$ are mutually inverse bijections.

$\square$

Because of [19], the matrix $\mathcal{M}^A_{t,k}$ of the previous theorem is called *Kramer Mesner matrix*. Equation (3.1) is the *Kramer Mesner system*. An efficient algorithm for solving this system is described by Wassermann in [29]. A program package for the constraction of designs with a prescribed automorphism group has been developed by the author. The program DISCRETA [3] is freely available over the Internet. Due to its graphical user interface it is easy to use. It runs on all Unix systems, especially on Linux. The program provides a large set of groups whch can be requested by pressing buttons. Groups can be combined and modified in various ways to obtaine new groups. The system is able to compute the Kramer Mesner matrix for reasonable parameters. The program of A. Wassermann is integrated into the system and can be used for solving the diophantine equations.

3.1.2 Example Consider the three dimensional cube with vertices numbered as in Figure 3.1. We are looking for designs with parameters 3-(8, 4, 1) where we



$1 = 000$	$5 = 001$
$2 = 100$	$6 = 101$
$3 = 010$	$7 = 011$
$4 = 110$	$8 = 111$

Figure 3.1: The Three Dimensional Space $GF(2)^3$ as Cube

take $\mathcal{V}$ to be the 8 vertices of the cube. The designs we are looking for shall be invariant under the group of the cube. This means that we choose the group A as the group of rotations of the group isomorphic to Sym_4 generated by the following two permutations:

$$\alpha = (1)(2, 3, 5)(6, 4, 7)(8),$$

$$\beta = (1, 2, 4, 3)(5, 6, 8, 7) .$$

We now compute the orbits $\mathcal{O}_{i,j}$ of this group A on i-subsets. We find the following number of orbits: $\ell_0 = 1$, $\ell_1 = 1$, $\ell_2 = 3$, $\ell_3 = 3$, $\ell_4 = 7$. Table 3.1 shows the

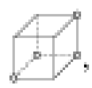
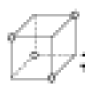
$\mathcal{O}_{0,1}$:	$\{\}_{24,1}$	$\mathcal{O}_{4,1}$:	$\{1, 2, 3, 4\}_{4,6}$
$\mathcal{O}_{1,1}$:	$\{1\}_{3,8}$	$\mathcal{O}_{4,2}$:	$\{1, 2, 3, 8\}_{1,24}$
$\mathcal{O}_{2,1}$:	$\{1, 2\}_{2,12}$	$\mathcal{O}_{4,3}$:	$\{1, 2, 3, 6\}_{2,12}$
$\mathcal{O}_{2,2}$:	$\{1, 8\}_{6,4}$	$\mathcal{O}_{4,4}$:	$\{1, 2, 3, 7\}_{2,12}$
$\mathcal{O}_{2,3}$:	$\{1, 4\}_{2,12}$	$\mathcal{O}_{4,5}$:	$\{1, 2, 3, 5\}_{3,8}$
$\mathcal{O}_{3,1}$:	$\{1, 2, 3\}_{1,24}$	$\mathcal{O}_{4,6}$:	$\{1, 2, 7, 8\}_{4,6}$
$\mathcal{O}_{3,2}$:	$\{1, 2, 7\}_{1,24}$	$\mathcal{O}_{4,7}$:	$\{1, 4, 6, 7\}_{12,2}$
$\mathcal{O}_{3,3}$:	$\{1, 4, 6\}_{3,8}$		

Table 3.1: The Orbits of the Group of the Cube

orbits and their representatives $O_{i,j}$. The order of the stabilizer and the length of the orbit are indicated in the index. We compute the matrix $\mathcal{M}^A_{3,4}$ which is shown in Figure 3.2. For each row and column of the matrix, we show the corresponding orbit on 3- and 4-subsets. In addition, we show the representing set as a subset of the vertex set of the cube for any t- and k-orbit. The system $\mathcal{M}^A_{3,4} \cdot \mathfrak{x}^\top = \underline{1}_{3\times 1}$ has exactly four solutions $\mathfrak{x}_i \in \{0, 1\}^7$, forming the set $\mathfrak{L}^A_{3-(8,4,1)}$:

$$\begin{aligned} \mathfrak{x}_1 &= (0, 0, 1, 0, 0, 0, 1), \\ \mathfrak{x}_2 &= (0, 0, 0, 1, 0, 0, 1), \\ \mathfrak{x}_3 &= (0, 0, 0, 0, 1, 1, 0), \\ \mathfrak{x}_4 &= (1, 0, 0, 0, 0, 1, 1). \end{aligned}$$

From this set of solutions, we get the corresponding designs $\mathcal{D}_{\mathfrak{x}_i} = (\mathcal{V}, \mathcal{B}_{\mathfrak{x}_i})$ for $i = 1, \ldots, 4$ forming the set $\mathfrak{D}^A_{3-(8,4,1)}$:

$\mathcal{D}_{\mathfrak{x}_1} = (\mathcal{V}, \mathcal{O}_{4,3} \cup \mathcal{O}_{4,7}) \qquad = (\mathcal{V};$ , ; $A)$,

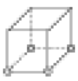
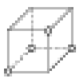
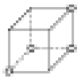
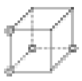
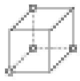
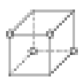
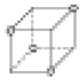
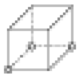
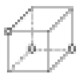
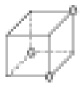
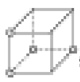
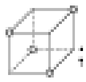
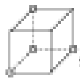
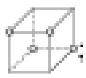
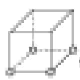
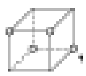
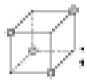
	 $\{1,2,3,4\}_{4,6}$	 $\{1,2,3,8\}_{1,24}$	 $\{1,2,3,6\}_{2,12}$	 $\{1,2,3,7\}_{2,12}$	 $\{1,2,3,5\}_{3,8}$	 $\{1,2,7,8\}_{4,6}$	 $\{1,4,6,7\}_{12,2}$
 $\{1,2,3\}_{1,24}$	1	1	1	1	1	0	0
 $\{1,2,7\}_{1,24}$	0	2	1	1	0	1	0
 $\{1,4,6\}_{3,8}$	0	3	0	0	1	0	1

Figure 3.2: The Kramer Mesner Matrix $\mathcal{M}^A_{3,4}$

$\mathcal{D}_{\xi_2} = (\mathcal{V}, \mathcal{O}_{4,4} \cup \mathcal{O}_{4,7}) = (\mathcal{V};$ , $; A)$,

$\mathcal{D}_{\xi_3} = (\mathcal{V}, \mathcal{O}_{4,5} \cup \mathcal{O}_{4,6}) = (\mathcal{V};$ , $; A)$,

$\mathcal{D}_{\xi_4} = (\mathcal{V}, \mathcal{O}_{4,1} \cup \mathcal{O}_{4,6}\mathcal{O}_{4,7}) = (\mathcal{V};$ , , $; A)$.

◇

Some of the most prominent t-designs have a Metheu group as group of automorphisms. They were constructed by Witt in [31]. Here the large Witt design for the Mathieu group M_{24} :

3.1.3 Example The group M_{24} is generated by the permutations

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

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

(1 24)(2 23)(3 12)(4 16)(5 18)(6 10)(7 20)(8 14)(9 21)(11 17)(13 22)(15 19).

and has 244823040 elements. One checks that the parameters 5-(24, 8, 1) are admissible. The orbits of this group on subsets of cardinality less than or equal to 8 are as follows (in the index we have the order of the stabilizer):

0-orbits :

1: $\{\}_{244823040}$

1-orbits :

1: $\{1\}_{10200960}$

2-orbits :

1: $\{1, 2\}_{887040}$

3-orbits :

1: $\{1, 2, 3\}_{120960}$

4-orbits :

1: $\{1, 2, 3, 4\}_{23040}$

5-orbits :

1: $\{1, 2, 3, 4, 5\}_{5760}$

6-orbits :

1: $\{1, 2, 3, 4, 5, 6\}_{2160}$

2: $\{1, 2, 3, 4, 5, 8\}_{11520}$

7-orbits :

1: $\{1, 2, 3, 4, 5, 6, 7\}_{720}$

2: $\{1, 2, 3, 4, 5, 8, 11\}_{40320}$

8-orbits :

1: $\{1, 2, 3, 4, 5, 6, 7, 8\}_{384}$

2: $\{1, 2, 3, 4, 5, 6, 7, 17\}_{2520}$

3: $\{1, 2, 3, 4, 5, 8, 11, 13\}_{322560}$

We obtain the following Kramer Mesner matrix. The rows and columns are labelled by orbit representatives:

$$\mathcal{M}_{5,8}^{M_{24}} = \begin{array}{cccc} & \{1, 2, 3, 4, 5, 6, 7, 8\}_{384, 637560} & \{1, 2, 3, 4, 5, 6, 7, 17\}_{2520, 97152} & \{1, 2, 3, 4, 5, 8, 11, 13\}_{322560, 759} \\ \{1, 2, 3, 4, 5\}_{5760, 42504} & \multicolumn{3}{l}{\begin{pmatrix} 840 & 128 & 1 \end{pmatrix}} \end{array}$$

The system $\mathcal{M}_{5,8}^{M_{24}} \cdot \mathfrak{x}^\top = (1)$ has the obvious solution $\mathfrak{x} = (0, 0, 1)$, i. e. the 759 elements of the orbit $\mathcal{O}_{8,3}$ form a block transitive 5-(24, 8, 1) Steiner System which is invariant under M_{24}. ◇

As every t-design with $t \geq 1$ is also a $(t-1)$-design, we get the following result from Theorem 3.1.1.

3.1.4 Corollary *Let $\mathfrak{x} \in \mathfrak{L}^A_{t-(v,k,\lambda)}$ be a solution vector for a t-(v, k, λ) design with prescribed automorphism group A. Then, for $i \leq t$,*

$$\mathcal{M}^A_{i,k} \cdot \mathfrak{x}^\top = \lambda_i \cdot \underline{1}_{\ell_i \times 1}. \tag{3.2}$$

In other words,

$$\mathfrak{x} \in \mathfrak{L}^A_{i-(v,k,\lambda_i)} \text{ for } i \leq t. \tag{3.3}$$

3.2 Construction of 8-(31, 10, λ) Designs

In 1998, the existence of 8-(31, 10, λ) designs could be proved (cf. [4]). These designs have been constructed using the method of Kramer and Mesner by prescribing the group PSL(3, 5). We take the 31 elements of PG(2, 5) : Let us describe the procedure briefly:

$1 \hat{=} (1,0,0)^\top$	$8 \hat{=} (1,0,1)^\top$	$15 \hat{=} (3,1,1)^\top$	$22 \hat{=} (0,3,1)^\top$	$29 \hat{=} (2,4,1)^\top$
$2 \hat{=} (0,1,0)^\top$	$9 \hat{=} (2,0,1)^\top$	$16 \hat{=} (4,1,1)^\top$	$23 \hat{=} (1,3,1)^\top$	$30 \hat{=} (3,4,1)^\top$
$3 \hat{=} (1,1,0)^\top$	$10 \hat{=} (3,0,1)^\top$	$17 \hat{=} (0,2,1)^\top$	$24 \hat{=} (2,3,1)^\top$	$31 \hat{=} (4,4,1)^\top$
$4 \hat{=} (2,1,0)^\top$	$11 \hat{=} (4,0,1)^\top$	$18 \hat{=} (1,2,1)^\top$	$25 \hat{=} (3,3,1)^\top$	
$5 \hat{=} (3,1,0)^\top$	$12 \hat{=} (0,1,1)^\top$	$19 \hat{=} (2,2,1)^\top$	$26 \hat{=} (4,3,1)^\top$	
$6 \hat{=} (4,1,0)^\top$	$13 \hat{=} (1,1,1)^\top$	$20 \hat{=} (3,2,1)^\top$	$27 \hat{=} (0,4,1)^\top$	
$7 \hat{=} (0,0,1)^\top$	$14 \hat{=} (2,1,1)^\top$	$21 \hat{=} (4,2,1)^\top$	$28 \hat{=} (1,4,1)^\top$	

The group PSL(3, 5) acts on these elements as a permutation group of degree 31. The group is generated by the following elements:

(1 2 6)(3 4 5)(8 12 16 11 27 28)(9 17 20 10 22 24)(13 21 15 31 23 29)(14 26 19 30 18 25),

(1 3 5 4 6)(8 13 18 23 28)(9 19 29 14 24)(10 25 15 30 20)(11 31 26 21 16),

(1 4 5 6)(8 21 18 16)(9 30 29 20)(10 14 15 24)(11 23 26 28)(12 17 27 22)(13 31)(19 25),

(1 7 27 6)(2 11)(3 9 22 15)(4 10 12 19)(5 8 17 23)(13 25 18 14)(16 31)(20 30 24 29).

The group is of order

$$\frac{(5^3-1)(5^3-5)(5^3-5^2)}{5-1} = (5^2+5+1)(5^2-1)(5-1)5^3 = 372000.$$

Table 3.2 shows the numbers of orbits of $A = \mathrm{PSL}(3,5)$ on i-subsets of $\mathcal{V} = \mathrm{PG}(2,5)$ for $i \leq 10$. The following table shows all 10-orbits of A on $\mathcal{V}$. We give the lexicographically minimal representative within each orbit. The stabilizer order of the representing set is indicated in the subscript. The orbit length is the index of the stabilizer in A. Each representative starts with the sequence of natural numbers 1, 2, 3, … For reasons of space, only the last element of this sequence is shown, the beginning is abbreviated by the symbol '…'. For instance, the set {1, 2, 3, 4, 5, 7, 16, 20, 24, 28} is displayed as {…, 5, 7, 16, 20, 24, 28}.

i	0	1	2	3	4	5	6	7	8	9	10
# i-orbits of A	1	1	1	2	3	5	12	22	42	92	174

Table 3.2: Numbers of Orbits of PSL(3, 5) on i-Subsets of PG(2, 5)

10-orbits:

1: $\{\ldots, 5, 7, 16, 20, 24, 28\}_{800}$

2: $\{\ldots, 10\}_{80}$

3: $\{\ldots, 5, 7, 8, 12, 21, 25\}_{4}$

4: $\{\ldots, 9, 12\}_{2}$

5: $\{\ldots, 5, 7, 8, 12, 16, 20\}_{2}$

6: $\{\ldots, 5, 7, 8, 12, 16, 24\}_{2}$

7: $\{\ldots, 5, 7, 8, 12, 14, 25\}_{1}$

8: $\{\ldots, 5, 7, 8, 9, 13, 17\}_{1}$

9: $\{\ldots, 5, 7, 8, 9, 13, 30\}_{2}$

10: $\{\ldots, 5, 7, 8, 12, 13, 21\}_{2}$

11: $\{\ldots, 5, 7, 8, 9, 12, 21\}_{2}$

12: $\{\ldots, 5, 7, 8, 9, 12, 29\}_{4}$

13: $\{\ldots, 8, 12, 13\}_{8}$

14: $\{\ldots, 8, 12, 14\}_{4}$

15: $\{\ldots, 8, 12, 19\}_{6}$

16: $\{\ldots, 5, 7, 8, 9, 12, 13\}_{1}$

17: $\{\ldots, 5, 7, 8, 9, 12, 28\}_{1}$

18: $\{\ldots, 5, 7, 8, 12, 14, 18\}_{2}$

19: $\{\ldots, 5, 7, 8, 12, 14, 28\}_{2}$

20: $\{\ldots, 5, 7, 8, 9, 13, 16\}_{2}$

21: $[\dots, 5, 7, 8, 9, 13, 28]_4$
22: $[\dots, 5, 7, 8, 12, 13, 20]_1$
23: $[\dots, 5, 7, 8, 9, 12, 24]_1$
24: $[\dots, 5, 7, 8, 9, 12, 17]_2$
25: $[\dots, 5, 7, 8, 12, 14, 24]_4$
26: $[\dots, 5, 7, 8, 9, 13, 20]_1$
27: $[\dots, 5, 7, 8, 9, 14, 18]_1$
28: $[\dots, 5, 7, 8, 9, 13, 15]_1$
29: $[\dots, 5, 7, 8, 12, 14, 19]_1$
30: $[\dots, 5, 7, 8, 9, 12, 22]_1$
31: $[\dots, 5, 7, 8, 9, 12, 14]_1$
32: $[\dots, 5, 7, 8, 9, 12, 18]_1$
33: $[\dots, 5, 7, 8, 9, 13, 22]_1$
34: $[\dots, 5, 7, 8, 9, 13, 14]_1$
35: $[\dots, 5, 7, 8, 9, 13, 27]_1$
36: $[\dots, 5, 7, 8, 9, 14, 31]_2$
37: $[\dots, 5, 7, 8, 9, 12, 27]_1$
38: $[\dots, 5, 7, 8, 9, 13, 23]_1$
39: $[\dots, 5, 7, 8, 9, 10, 12]_2$
40: $[\dots, 5, 7, 8, 9, 10, 15]_8$
41: $[\dots, 5, 7, 8, 9, 14, 19]_2$
42: $[\dots, 5, 7, 8, 9, 14, 27]_4$
43: $[\dots, 5, 7, 8, 9, 14, 15]_2$
44: $[\dots, 5, 7, 8, 13, 15, 22]_{20}$
45: $[\dots, 4, 7, 8, 12, 16, 20, 28]_2$
46: $[\dots, 4, 7, 8, 12, 16, 20, 24]_4$
47: $[\dots, 4, 7, 8, 12, 16, 21, 25]_2$
48: $[\dots, 4, 7, 8, 12, 14, 25, 29]_1$
49: $[\dots, 4, 7, 8, 9, 12, 19, 26]_1$
50: $[\dots, 4, 7, 8, 9, 12, 19, 28]_1$
51: $[\dots, 4, 7, 8, 12, 13, 21, 29]_2$
52: $[\dots, 4, 7, 8, 9, 12, 18, 24]_2$
53: $[\dots, 4, 7, 8, 9, 12, 18, 30]_2$
54: $[\dots, 4, 7, 8, 12, 15, 18, 26]_8$
55: $[\dots, 4, 7, 8, 12, 21, 25, 26]_{16}$
56: $[\dots, 4, 7, 8, 12, 16, 20, 29]_4$
57: $[\dots, 4, 7, 8, 12, 16, 20, 25]_1$
58: $[\dots, 4, 7, 8, 12, 16, 20, 21]_2$
59: $[\dots, 4, 7, 8, 12, 15, 19, 29]_1$
60: $[\dots, 4, 7, 8, 9, 13, 20, 26]_2$
61: $[\dots, 4, 7, 8, 9, 12, 20, 29]_1$
62: $[\dots, 4, 7, 8, 9, 13, 20, 21]_1$
63: $[\dots, 4, 7, 8, 12, 15, 19, 23]_1$
64: $[\dots, 4, 7, 8, 9, 12, 16, 20]_2$
65: $\{\dots, 4, 7, 8, 9, 12, 13, 29\}_1$
66: $\{\dots, 4, 7, 8, 12, 16, 19, 29\}_1$
67: $\{\dots, 4, 7, 8, 9, 12, 19, 23\}_2$
68: $\{\dots, 4, 7, 8, 9, 12, 16, 17\}_1$
69: $\{\dots, 4, 7, 8, 9, 12, 13, 21\}_1$
70: $\{\dots, 4, 7, 8, 9, 12, 16, 29\}_2$
71: $\{\dots, 4, 7, 8, 12, 16, 19, 20\}_2$
72: $\{\dots, 4, 7, 8, 12, 15, 23, 29\}_2$
73: $\{\dots, 4, 7, 8, 9, 13, 20, 24\}_1$
74: $\{\dots, 4, 7, 8, 9, 12, 20, 26\}_6$
75: $\{\dots, 4, 7, 8, 9, 12, 17, 20\}_1$
76: $\{\dots, 4, 7, 8, 12, 19, 20, 23\}_2$
77: $\{\dots, 4, 7, 8, 9, 12, 18, 29\}_1$
78: $\{\dots, 4, 7, 8, 12, 16, 19, 23\}_2$
79: $\{\dots, 4, 7, 8, 12, 16, 21, 28\}_2$
80: $\{\dots, 4, 7, 8, 9, 12, 18, 26\}_1$
81: $\{\dots, 4, 7, 8, 9, 12, 18, 20\}_1$
82: $\{\dots, 4, 7, 8, 9, 13, 17, 20\}_1$
83: $\{\dots, 4, 7, 8, 9, 12, 18, 31\}_1$
84: $\{\dots, 4, 7, 8, 9, 12, 20, 24\}_1$
85: $\{\dots, 4, 7, 8, 12, 13, 20, 24\}_1$
86: $\{\dots, 4, 7, 8, 9, 12, 19, 31\}_1$
87: $\{\dots, 4, 7, 8, 9, 12, 13, 20\}_1$
88: $\{\dots, 4, 7, 8, 9, 12, 16, 19\}_1$
89: $\{\dots, 4, 7, 8, 12, 13, 21, 24\}_1$
90: $\{\dots, 4, 7, 8, 9, 12, 13, 18\}_1$
91: $\{\dots, 4, 7, 8, 12, 13, 21, 26\}_1$
92: $\{\dots, 4, 7, 8, 9, 12, 21, 24\}_2$
93: $\{\dots, 4, 7, 8, 9, 12, 15, 29\}_1$
94: $\{\dots, 4, 7, 8, 9, 13, 17, 28\}_1$
95: $\{\dots, 4, 7, 8, 9, 12, 15, 20\}_1$
96: $\{\dots, 4, 7, 8, 12, 14, 28, 29\}_1$
97: $\{\dots, 4, 7, 8, 9, 12, 19, 20\}_1$
98: $\{\dots, 4, 7, 8, 12, 14, 18, 29\}_1$
99: $\{\dots, 4, 7, 8, 9, 17, 20, 25\}_1$
100: $\{\dots, 4, 7, 8, 9, 12, 16, 28\}_2$
101: $\{\dots, 4, 7, 8, 9, 12, 13, 17\}_1$
102: $\{\dots, 4, 7, 8, 9, 17, 19, 23\}_1$
103: $\{\dots, 4, 7, 8, 9, 12, 15, 27\}_2$
104: $\{\dots, 4, 7, 8, 9, 12, 18, 19\}_1$
105: $\{\dots, 4, 7, 8, 9, 17, 18, 26\}_2$
106: $\{\dots, 4, 7, 8, 9, 12, 17, 26\}_3$
107: $\{\dots, 4, 7, 8, 9, 17, 19, 26\}_1$
108: $\{\dots, 4, 7, 8, 9, 12, 15, 28\}_1$
109: $[\dots, 4, 7, 8, 9, 12, 15, 21]_1$
110: $[\dots, 4, 7, 8, 9, 12, 19, 24]_1$
111: $[\dots, 4, 7, 8, 9, 12, 18, 27]_1$
112: $[\dots, 4, 7, 8, 9, 17, 20, 23]_1$
113: $[\dots, 4, 7, 8, 9, 12, 15, 17]_1$
114: $[\dots, 4, 7, 8, 9, 12, 20, 21]_1$
115: $[\dots, 4, 7, 8, 9, 12, 20, 28]_1$
116: $[\dots, 4, 7, 8, 9, 12, 14, 20]_1$
117: $[\dots, 4, 7, 8, 9, 13, 21, 27]_1$
118: $[\dots, 4, 7, 8, 9, 12, 28, 31]_2$
119: $[\dots, 4, 7, 8, 9, 12, 19, 21]_1$
120: $[\dots, 4, 7, 8, 9, 12, 14, 19]_1$
121: $[\dots, 4, 7, 8, 9, 12, 21, 31]_1$
122: $[\dots, 4, 7, 8, 9, 12, 15, 18]_1$
123: $[\dots, 4, 7, 8, 9, 13, 14, 17]_1$
124: $[\dots, 4, 7, 8, 9, 12, 13, 19]_1$
125: $[\dots, 4, 7, 8, 9, 14, 17, 25]_2$
126: $[\dots, 4, 7, 8, 12, 14, 25, 28]_1$
127: $[\dots, 4, 7, 8, 9, 12, 14, 28]_1$
128: $[\dots, 4, 7, 8, 9, 13, 21, 24]_2$
129: $[\dots, 4, 7, 8, 9, 12, 17, 18]_1$
130: $[\dots, 4, 7, 8, 9, 12, 18, 25]_2$
131: $[\dots, 4, 7, 8, 9, 12, 27, 28]_1$
132: $[\dots, 4, 7, 8, 9, 12, 13, 28]_1$
133: $[\dots, 4, 7, 8, 9, 12, 15, 19]_1$
134: $[\dots, 4, 7, 8, 9, 12, 14, 18]_1$
135: $[\dots, 4, 7, 8, 9, 12, 19, 27]_1$
136: $[\dots, 4, 7, 8, 9, 12, 18, 21]_1$
137: $[\dots, 4, 7, 8, 12, 13, 20, 21]_1$
138: $[\dots, 4, 7, 8, 12, 20, 21, 28]_4$
139: $[\dots, 4, 7, 8, 9, 13, 17, 21]_1$
140: $[\dots, 4, 7, 8, 12, 14, 18, 25]_1$
141: $[\dots, 4, 7, 8, 9, 13, 18, 20]_2$
142: $[\dots, 4, 7, 8, 9, 13, 14, 20]_1$
143: $[\dots, 4, 7, 8, 9, 13, 15, 20]_2$
144: $[\dots, 4, 7, 8, 12, 14, 24, 25]_2$
145: $[\dots, 4, 7, 8, 9, 12, 14, 21]_1$
146: $[\dots, 4, 7, 8, 12, 15, 18, 21]_2$
147: $[\dots, 4, 7, 8, 9, 13, 14, 18]_1$
148: $[\dots, 4, 7, 8, 9, 13, 15, 17]_2$
149: $[\dots, 4, 7, 8, 12, 13, 24, 26]_4$
150: $[\dots, 4, 7, 8, 9, 14, 17, 18]_2$
151: $[\dots, 4, 7, 8, 9, 12, 13, 27]_2$
152: $[\dots, 4, 7, 8, 12, 15, 19, 20]_4$

153: $[\dots, 4, 7, 8, 9, 13, 15, 27]_4$
154: $[\dots, 4, 7, 8, 12, 13, 20, 30]_2$
155: $[\dots, 4, 7, 8, 9, 12, 13, 15]_2$
156: $[\dots, 4, 7, 8, 9, 13, 15, 28]_2$
157: $[\dots, 4, 7, 8, 9, 12, 14, 16]_4$
158: $[\dots, 4, 7, 8, 9, 12, 16, 27]_8$
159: $[\dots, 4, 7, 8, 9, 12, 13, 16]_6$
160: $[\dots, 4, 7, 8, 9, 12, 13, 14]_6$
161: $[\dots, 4, 7, 8, 9, 13, 14, 27]_6$
162: $[\dots, 4, 7, 8, 9, 14, 17, 21]_3$
163: $[\dots, 4, 7, 8, 9, 12, 14, 27]_2$
164: $[\dots, 4, 7, 8, 12, 14, 18, 19]_4$
165: $[\dots, 4, 7, 8, 9, 12, 14, 15]_2$
166: $[\dots, 4, 7, 8, 9, 13, 18, 25]_{20}$
167: $[\dots, 4, 7, 8, 9, 13, 14, 15]_{12}$
168: $[\dots, 3, 7, 8, 12, 15, 19, 20, 23]_2$
169: $[\dots, 3, 7, 8, 12, 13, 20, 21, 24]_5$
170: $[\dots, 3, 7, 8, 12, 14, 21, 24, 28]_2$
171: $[\dots, 3, 7, 8, 12, 14, 21, 28, 31]_4$
172: $[\dots, 3, 7, 8, 12, 15, 19, 21, 26]_{24}$
173: $[\dots, 3, 7, 8, 12, 14, 18, 21, 31]_5$
174: $[\dots, 3, 7, 8, 13, 21, 24, 29, 30]_{120}$

Tables 3.3 and 3.4 show the (42×174)-Kramer Mesner matrix $\mathcal{M}_{8,10}^{\mathrm{PSL}(3,5)}$. In order to display every entry with just one character, we substitute numbers larger than 9 by small letters:

$$a \hat{=} 10, \quad b \hat{=} 11, \quad c \hat{=} 12, \dots .$$

The numbers 40, 60 and 120 are represented by capital letters A, B and C, respectively.

We find designs for $\lambda = 93$ and $\lambda = 100$. More precisely, the solution sets have the following cardinalities:

$$|\mathfrak{L}^{A}_{8-(31,10,93)}| = 138,$$
$$|\mathfrak{L}^{A}_{8-(31,10,100)}| = 1658.$$

Any solution vector $\mathfrak{x} \in \mathfrak{L}^{A}_{8-(31,10,\lambda)}$ gives rise to a design $\mathcal{D}_{\mathfrak{x}} = (\mathcal{V}, \mathcal{B}_{\mathfrak{x}})$ in the way described in Theorem 3.1.1. We specify the designs by simply listing the set of indices j with $\mathfrak{x}(j) = 1$. The first three designs in the case $\lambda = 93$ are:

$\mathcal{D}_{\mathfrak{x}_1}$: 1, 2, 5, 7, 9, 12, 13, 14, 16, 19, 24, 25, 29, 30, 33, 36, 39, 42, 43, 46, 48, 52, 53, 55, 57, 60, 64, 65, 72, 75, 76, 81, 83, 84, 85, 91, 92, 94, 96, 98, 103, 105, 107, 109, 113, 114, 116, 120, 124, 125, 126, 128, 131, 132, 136, 138, 139, 141, 147, 148, 149, 150, 152, 159, 162, 167, 168, 172.

$\mathcal{D}_{\mathfrak{x}_2}$: 1, 2, 5, 7, 9, 12, 13, 14, 16, 19, 24, 25, 29, 30, 35, 36, 39, 42, 43,

```
12AkkkAAkkka..........................................................................
.3.c........uBA.......................................................................
..3999cc6663364cc6663cc63c6666666663666...............................................
...9..64232136466443106226ccmacccccc6ga638491.........................................
.3.k...84.42...88..44.88.888.g888884ggw8844...........................................
12A..................................g4....g8gwwwggg42................................
..3122463221...13..11.21.3.1.1.1112.122.....422b84424..1315161223313121331417114213422323l
..3122442242...22.....42.2...2222...2.2.....422884724..1222262222622224.2121.1.42224..424.
..3122442221....1.....1..121.21331312211211.21544a25221.21.1.1..2.121...2.1.2.233423141312
....84.....21..884446.......................84......4..6848cg88488888844848484............
....2423.....1.1.111.5642631132111..........312151.....142316433221331124272311341442l4212
....42...2.11..c622214.....4.....6.3........222...1.2..1422242246429462.2.2.222442422440 26
...2...84......44..46.44.8.4.4..444.484..1......84..........c44.2........444....444.4.44...
......21221...1.522..43..23.42.23.5333..........133111.....12.42.1122311.4.3211.2.123132222
......42.....1.3.223.23.2363225334..............222........121531212.5..14.3111..332.223114
......4.2.11..1.6.4.14...4..4..4..6642...1.....222.22.....2.2.2.4.26.2.1..2.4..2224.242..4
...2...42.42...66..22.67.4.2.844222.644.........42.24.......4..24.1g23...10.4..22.22.224.2
.........431..1.44..144..26.4..24.4.24...1........244.......22.142.4421.2.2.42.22.422.2424
....42..2...1..442241......24.6..44.22...14.2.4.22......22.2.2..2........2.2...322222.4.2..
....24....4..1.......44214.44..44...44..2.21.24....44...4...........84.......4.44444444448
......23.....1.2.111.11.1137533662......4.31...115..........1.2..1.1.....1.1.1...16..1311..
...2...21.21...33..11.34.243.844333288831522.....12.21......1.1....141...1.3.1..11111.5.1.6
......42..2..1.4.223.22.2242226222..22....1....4...222....2..222...622.1....2..42.22...6.2
...2...42......22..22.22.444.6224442mm31422.....24..........1.2..2...2...2.2........22..42..4
.........2.11..6.....4.....64.8..g63.....16.......12.............4...4.......2.......2.4.26
......22321...1.422..422.22.4..22.4244..2.......2442..11....14..222..2...212..1.44424282224
.........4.21..8...4.8.....g......8.4.................4...2....4.8.........4...84....88.8.8.....
...2.................1.....84.c44444488822m64...........................................
...........21.................8.8..g8......6c.........4...................................8
....2..........2.22..2..3........2..........211........3456248g56g32c2234..3.4326.2.2.24.2
.....222...........2..21.2....2..............3.144......363c.8.63.2.....7424845122.246.6.2.
.....2...4.......4..........4.......4.........22...4.2.218.........424.242....446488484844c4
....2.4..........1.........4.2..222.........2.1.34.2...2..23...2..2.1.....2.....8422..2..4..
......22..........21..31..1..31.11.................422.........612541323.2.234.2442..1413614331
......22.2........1.....2...2..22.22....1..1....4.421..1...2..2212.2.2..22...2...4c.424..2.
......3.111.....1.1..12..12.1...1.1.1............4212111....5.226.27.141113.2211.3.142313391
....4...........8..................................44..........m8c8488cc8g488cc.................8..
....13...............2..2.....22.4..2..........314...........c82...2.2..2.1..2...2.562244622222
....111.111....111...1...1.11.11..1..1....1.112211211..162213121271221212...32353163612282
.........2.2....4.2.14.............................4.4.....8.444.44.4.cm2..4644.4..444.444.
....22..........2.1.2.2.....2.....2..........422.........4i462642248222136414447428422422422
.........2.2..........4......8.....4......1........44..............4...4.6.....8.......8.4.84
```

Table 3.3: $\mathcal{M}_{8,10}^{PSL(3,5)}$, Left Part

```
.................................................................................
.................................................................................
.................................................................................
.................................................................................
.................................................................................
.................................................................................
115111342111242123121111313121211213222111111....................................
.2..4.22.......2..44.228842.2.4...24.221.22222212212412..........................
21123221122212114332241123223255211111.33511114112212112333......................
..8.............................8.......................24.......................
21125251314 2.1.3.112..54552.12...1.2124..1513.2132111......12111................
242422226444.........2.2..........42..2...62.2.2..22.........21.1322231..........
...84.4.4.....244444444448................4..4.....442...........442.............
22221122411322214354333222414321452.32113422522.11122.2.1.12211..1.1..1111.......
1.3532312.5.111.1333.23223413412252232 2..25441..2132113.3.133..1322.11.12.2.....
.242222.42.6321..4..42222242.222.42462422824.22.42.6124.2..12122.2.1..1..........
.14.2.2..26.32.2.4422.8222.12222.6..2.63222222........2.....1...1.1121..1.1......
2224...22.24141.24422242.44.2422222.22422224444.4224..2.2..21.12.2.....211.......
..6642424222222268424442 42.2..46...22.222442242242 22.22.2......1421.1..2.13....
44..........44..44484444....4.444...4.46...4.8.1..2..24.422................1.....
..1411211.53.51.222252.11422273383212.2.6214521.5124329.56.2..11341..113413.1....
.1.4..1.2.4312112335927 1.21.2411121..162431132..2.23..4.62.12...2411...23.31....
.24.64.22422341.44824.42....4.48.2....444242262.24.2..244..131..2.112..2114......
..242....12.3....4448.a.2622.22224..21.2662.6...2.262.2.45..3.1.23.1111.2.111....
2.........66242.4..462.2.44.46..46..8.6.66.4.42.4..a..6.8.124.213.2.13224.8.1....
4.24222.222.2.224226444242.42.442..24..34222.2..222..124651....2...........1.....
8..8..8.8.............8.8...8..................g.....4.8..4.c...24.c84.........2.
...4......4.2....44.c.4..44..c..482.4...44.44.....28..c.4..22.1..a11.244i.2.1....
............8..4......8......8g..g.....8.g..........o4...g..44.....2..48.g28.4...
21426a224462...........2.........4......26...2..61.......2532.21...11.......92421..
2.6.6.662...1212.22...26622.2..2...6222...62..6226...1...........1...1.....1..9454.2.
c8.....44..4.........8.....8......6..6...4..4.4.....2..a.61...1222.1......3..1.46.1..
..224a262322.21.644..4....6144a88262...34..426222824252a4..3.....1...112231.1.....2.
6.5122473.13151.2222.2.33221322312144 12..134325.5413221.1.22.124.......1.2...3242.1.
6.222628..22183.2...24..22844264c2244...4222.22.42.2288526.11.12......1..1.....21.2.
2321272513.1121.4133.123515351543116441222321 43.23...3152.1.11.1...............314213.
.....8...4......................................................2..6.4..214........o.421.1
222246422224.232.......464.122.2.2.84.4..246..856a.2.22.2..32214..2..1..1.3....12.4.
51111.123.121321731324.1312.2.331.1a3121111417633511121.1.1....11......1.12...321.6.
444.444442.4.........4.8..........42..2...44.4.8..4..4.....2.2712.........1...c442..1
a12422448122.........2.2.....................2.2.2..22.1.....1..215412......1...3672...
8..........g244.4..4.c.8.44.88..c...8.4.8..4.48.4..48...4.44..24......2..4....4.....
```

Table 3.4: $\mathcal{M}_{8,10}^{\mathrm{PSL}(3,5)}$, Right Part

46, 49, 52, 53, 55, 57, 60, 63, 69, 70, 72, 75, 78, 80, 84, 85, 90, 94, 95, 98, 100, 101, 103, 104, 105, 110, 116, 117, 121, 122, 125, 128, 130, 134, 135, 137, 138, 139, 143, 147, 148, 149, 152, 156, 159, 163, 167, 169, 170, 172.

$\mathcal{D}_{\beta_3}$: 1, 2, 5, 8, 11, 12, 13, 14, 17, 19, 24, 25, 28, 29, 33, 36, 39, 42, 43, 46, 47, 48, 52, 55, 58, 60, 62, 64, 66, 71, 75, 76, 77, 78, 81, 85, 88, 90, 94, 97, 98, 105, 109, 111, 113, 116, 118, 119, 120, 125, 126, 127, 131, 132, 133, 136, 138, 140, 145, 146, 149, 151, 152, 159, 167, 169, 172.

3.3 List of t-Designs with Large t

In this section, some existens results for t-designs with large t shall be collected. If nothing else is stated, the results have been obtained in the research group around Prof. Dr. R. Laue at the University of Bayreuth.

At the beginning, we need a list of permutation group of moderate degree. A list of primitive groups of degree up to 50 can be found in the section "Finite Groups and Designs" of Chouinard II, Jajacay and Magliveras in the "Handbook of Combinatorial Designs" of Colbourn and Dinitz [9, pages 587-614].

Another source for groups is the ATLAS of group representations of Robert A. Wilson et al. [30].

parameters	group A, $\|A\|$, size of $\mathcal{M}^A_{t,k}$, solutions for
8-(40,11,1440)	$PSL(4,3)$, 6065280, 53×569, ($\Delta\lambda = 40$)
8-(36,11,1260)	$Sp(6,2)$, 1451520, 79×694, ($\Delta\lambda = 84$)
8-(31,10,λ)	$PSL(3,5)$, 372000, 42×174, $\lambda = 93$, 100 [4] ($\Delta\lambda = 1$)
8-(28,14,λ)	$ASL(3,3)+$, 151632, 48×352, $\lambda = 14040$, 18600 ($\Delta\lambda = 60$)
8-(28,13,λ)	$ASL(3,3)+$, 151632, 48×330, $\lambda = 5832$, 7080, 7128 ($\Delta\lambda = 24$)
8-(27,13,λ)	$ASL(3,3)$, 151632, 31×176, $\lambda = 3204$, 3240, 4608, 5076, 5148 ($\Delta\lambda = 18$)
8-(27,12,λ)	$ASL(3,3)$, 151632, 31×154 $\lambda = 1296$, 1932 ($\Delta\lambda = 6$)
8-(27,11,432)	$ASL(3,3)$, 151632, 31×121 ($\Delta\lambda = 3$)

Table 3.5: 8-Designs With Prescribed Automorphism Group

parameters	group A, $\|A\|$, size of $\mathcal{M}^A_{t,k}$, solutions for
7-(40,11,λ)	PSL(4, 3), 6065280, 24×569, $\lambda = 8250$, 11220, 14190, 14850, 17820 ($\Delta\lambda = 330$)
7-(40,10,λ)	PSL(4, 3), 6065280, 24×263, $\lambda = 560$, 1008, 1208, 1296, 1568, 1656, 2304, 2504 ($\Delta\lambda = 4$)
7-(36,11,λ)	Sp(6, 2), 1451520, 37×694, $\lambda = 3360$, 4200, 4536, 4935, 5040, 5271, 5376, 5775, 5880, 6111, 6216, 6615, 6720, 7056, 7455, 7560, 7791, 7896, 8295, 8400, 8631, 8736, 9135, 9240, 9471, 9576, 9975, 10080, 10311, 10416, 10815, 10920, 11151, 11655, 11760 ($\Delta\lambda = 21$)
7-(34,9,λ)	PΓL(2, 32)+, 163680, 45×345, $\lambda =$135, 171 ($\Delta\lambda = 9$)
7-(33,10,λ)	PΓL(2, 32), 163680, 32×596, $\lambda = 600$, 720, 840, 880 ($\Delta\lambda = 40$)
7-(33,9,λ)	PΓL(2, 32), 163680, 32×248, $\lambda = 60$, 65, 80, 85, 100, 105, 120, 125, 140, 145, 160 ($\Delta\lambda = 5$)
7-(33,8,10)	PΓL(2, 32), 163680, 32×97, ($\Delta\lambda = 2$)
7-(31,10,λ)	PSL(3, 5), 372000, 22×174, $\lambda =$480, 744, 800 ($\Delta\lambda = 8$)
7-(30,9,λ)	PΓL(2, 27) ++, 58968, 61×307, $\lambda =$105, 112 [5] ($\Delta\lambda = 1$)
7-(29,11,λ)	PΓL(2, 27)+, 58968, 43×647, $\lambda =$2130, 3465 ($\Delta\lambda = 385$)
7-(29,10,420)	PΓL(2, 27)+, 58968, 43×391, [5] ($\Delta\lambda = 140$)
7-(28,14,λ)	Sp(6, 2), 1451520, 16×103, $\lambda = 23040$, 30240,32760, 35280, 37800, 38160, 40320, 40680, 42840, 43200, 45720, 48240, 50760, 52920, 53280, 55440, 55800, 57960 ($\Delta\lambda = 180$)

Table 3.6: 7-Designs With Prescribed Automorphism Group (Part 1)

parameters	group A, $\lvert A\rvert$, size of $\mathcal{M}_{t,k}^A$, solutions for
7-(28,14,λ)	AGL(3, 3)+, 303264, $\times$ λ = 30420, 44460, 51480 [26] ($\Delta\lambda = 180$)
7-(28,13,λ)	Sp(6, 2), 1451520, 16 $\times$ 101, λ = 10080, 15120, 17640, 18984, 20160, 21504, 22680, 24024, 25200, 26544 ($\Delta\lambda =$ 84)
7-(28,13,24780)	AGL(3, 3)+, 303264, 26 $\times$ 241 ($\Delta\lambda = 84$)
7-(28,10,630)	PΓL(2, 27), 58968, 29 $\times$ 257, [5] ($\Delta\lambda = 70$)
7-(27,13,λ)	AGL(3, 3), 303264, 16 $\times$ 127 λ = 10140, 14820, 17160 [26] ($\Delta\lambda = 60$)
7-(27,12,λ)	ASL(3, 3), 151632, 17 $\times$ 154, λ = 1896, 1944, 5832, 7080, 7128, 8376 ($\Delta\lambda = 24$)
7-(27,12,λ)	AGL(3, 3), 303264, 16 $\times$ 114 λ = 2544, 2592, 3192, 3840, 3888, 4536, 5136, 5184, 6432, 6480, 7728 [26] ($\Delta\lambda = 24$)
7-(27,11,λ)	ASL(3, 3), 151632, 17 $\times$ 121, λ = 540, 675, 765, 810, 840, 900, 930, 945, 1035, 1080, 1110, 1170, 1200, 1335, 1380, 1515, 1650, 1755, 1875, 1890, 2010, 2115, 2250 ($\Delta\lambda = 15$)
7-(27,11,λ)	AGL(3, 3), 303264, 16 $\times$ 91 λ = 1215, 1305, 1350, 1440, 1470, 1485, 1575, 1605, 1620, 1710, 1740, 1785, 1845, 1920, 1980, 2025, 2055, 2145, 2160, 2190, 2280, 2295, 2325, 2385, 2415 [26] ($\Delta\lambda = 15$)
7-(27,11,λ)	U(4, 2), 25920, 77 $\times$ 668, λ = 1500, 1860, 2385, 2400 ($\Delta\lambda = 15$)
7-(27,10,λ)	PΓL(2, 25)+, 31200, 53 $\times$ 355, λ =240, 540 [5] ($\Delta\lambda = 60$)
7-(27,10,420)	U(4, 2), 25920, 77 $\times$ 458, ($\Delta\lambda = 60$)

Table 3.7: 7-Designs With Prescribed Automorphism Group (Part 2)

parameters	group A, $\lvert A\rvert$, size of $\mathcal{M}^A_{t,k}$, solutions for
7-(26,8,6)	PGL(2, 25), 15600, 54 × 131, [6] ($\Delta\lambda = 1$)
7-(26,9,λ)	PΓL(2, 25), 31200, 34 × 132, λ =54, 63, 81 [6] ($\Delta\lambda = 9$)
7-(26,11,λ)	PΓL(2, 25), 31200, 34 × 293, λ = 1176, 1356, 1536, 1716, 1896, 1926 ($\Delta\lambda = 6$)
7-(26,12,5796)	PΓL(2, 25), 31200, 34 × 379 ($\Delta\lambda = 18$)
7-(24,8,λ)	PSL(2, 23), 6072, 57 × 143, λ =4, 5, 6, 7, 8 [6] ($\Delta\lambda = 1$)
7-(24,9,λ)	PGL(2, 23), 12144, 36 × 125, λ =40, 48, 64 [6] ($\Delta\lambda = 4$)
7-(24,10,λ)	PGL(2, 23), 12144, 36 × 196, λ =240, 320, 340 [5],[20] ($\Delta\lambda = 20$)
7-(22,11,λ)	PGL(2, 19)++, 6840, 49 × 154, λ =315, 630 ($\Delta\lambda = 105$)
7-(20,10,λ)	PSL(2, 19), 3420, 26 × 74, λ =116, 124, 134 [5] ($\Delta\lambda = 2$)
7-(20,10,126)	$\big(\mathrm{PGL}(2, 8) \times C_2\big)++$, 1008, 111 × 244, ($\Delta\lambda = 2$)

Table 3.8: 7-Designs With Prescribed Automorphism Group (Part 3)

Chapter 4

The Plesken Ring

In his 1982 work "Counting with Groups and Rings", Plesken [23] was looking at groups acting on lattices, or – more generally – on semigroups. He was counting the number of certain equations within semigroups where the variables should belong to fixed orbits of the group.

4.1 Groups Acting on Lattices

Let us start by introducing the general concept of a *semigroup action*. Let A be a group and $(M, \circ)$ a semigroup. A acts on M if

$$(x \circ y)^a = x^a \circ y^a$$

for all $x, y \in M$ and all $a \in A$. In this case we calle thr group action of A on M *compatible* with the semigroup structure.

A *partial ordering* (poset) on a set P is a relation $\leq$ with

(PO1) $x \leq x$,

(PO2) $x \leq y$ and $y \leq x \Rightarrow x = y$,

(PO3) $x \leq y$ and $y \leq z \Rightarrow x \leq z$

for all $x, y, z \in P$. A subset $M \subseteq P$ all of whose elements are comparable, i. e. for which either $x \leq y$ or $y \leq x$ holds for all $x, y \in M$ is called *totally ordered* or *chain*. A subset $M \subseteq P$ in which no two elementa are comparable is called *antichain*.

A group A *acts on the poset* $(P, \leq)$, if

$$x \leq y \Rightarrow x^a \leq y^a$$

is satisfied for all $x, y \in P$ and all $a \in A$.

Let now $(P, \leq)$ be a poset and let M be a subset of P. An *upper (lower) bound* of M is an element w with $m \leq w$ ($m \geq w$) for all $m \in M$.

The *least upper bound* M is an upper bound w with the property that $w \leq w'$ for any other upper bound w' holds. This element is also called *supremum* of M. If the supremum of a set exists then it is unique,

The *greatest lower bound* of M is a lower bound w with the property that $w \geq w'$ for any other lower bound w'. This element is also called *infimum* of M. If the infimum of a set exists then it is unique.

If the supremum of a set M exists, we denote it as $\bigvee_{m \in M} m$ or $\bigvee M$. We write $x \vee y$ for the supremum of two elements x and y. If the infimum of a set M exists, we denote it as $\bigwedge_{m \in M} m$ or $\bigwedge M$. We write $x \wedge y$ for the infimum of two elements x and y.

A set P is called *lattice* if:

(L0a) $(P, \leq)$ is a poset,

(L0b) Any two elements of P have an infimum and a supremum.

A *complete lattice* is a lattice in which any subset has a supremum and an infimum. Any finite lattice is complete.

The following remark characterizes the operations $\vee$ and $\wedge$:

4.1.1 Remark Let $(\mathcal{L}, \vee, \wedge)$ be a lattice. Then for all $x, y, z \in \mathcal{L}$:

(L1) $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$ (commutativity),

(L2) $(x \vee y) \vee z = x \vee (y \vee z)$ and $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ (associativity),

(L3) $x \vee x = x$ and $x \wedge x = x$ (idempotency),

(L4) $(x \vee y) \wedge x = x$ and $(x \wedge y) \vee x = x$ (law of absorption).

On the other hand, any set M admitting two binary compositions $\vee$ and $\wedge$ satisfying (L1)-(L4) gives rise to a lattice:

4.1.2 Remark Let M be set admitting two binary compositions $\vee$ and $\wedge$ satisfying (L1)-(L4). The M is a lattice with respect to the partial order

$$x \leq y \ :\Longleftrightarrow \ x \vee y = y \quad \big(\Longleftrightarrow \ x \wedge y = x \big) \tag{4.1}$$

for all $x, y \in M$.

Summarizing this implies the equivalence

$$(L0a) \wedge (L0b) \iff (L1) \wedge (L2) \wedge (L3) \wedge (L4).$$

This means that we can specify either the ordering or the compositions $\vee$ and $\wedge$ of a lattice. We write $(M, \leq)$ or $(M, \vee, \wedge)$.

A *lattice action* is a group A acting on the set of elements of a lattice $(\mathcal{L}, \vee, \wedge)$ which is compatible with the operators supremum and infimum, i. e. which satisfies

$$(x \vee y)^a = x^a \vee y^a \qquad \text{and} \qquad (x \wedge y)^a = x^a \wedge y^a$$

for all $x, y \in \mathcal{L}$ and all $a \in A$.

4.1.3 Remark Let $(\mathcal{L}, \vee, \wedge)$ be a lattice and the $\leq$ be the ordering of the lattice. Let A be a group acting on the element of $\mathcal{L}$. Then the following statements are equivalent:

(i) A acts on $\mathcal{L}$ as a lattice action, i. e. $(x \vee y)^a = x^a \vee y^a$ and $(x \wedge y)^a = x^a \wedge y^a$ for all $x, y \in \mathcal{L}$, $a \in A$.

(ii) A acts on the poset $(\mathcal{L}, \leq)$ (i. e. $x \leq y \Rightarrow x^a \leq y^a$ for all $x, y \in \mathcal{L}$, $a \in A$).

Proof: Kerber [13, Lemma 5.1.11, page 145]. □

Let us now consider the action of the group A on the finite semigroup $(M, \circ)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ be the set of orbits of A on M. Moreover, let $o_1, \ldots, o_\ell$ be representing elements for the orbits, i. e. $o_i \in \mathcal{O}_i$ for $1 \leq i \leq \ell$. For $1 \leq i, j, k \leq \ell$, we put

$$\alpha^{\circ}_{ijk} := |\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \circ y = o_k\}|. \tag{4.2}$$

These numbers are independent of the choice of the representing sets $o_k \in \mathcal{O}_k$. For, let o_k^a be another element in $\mathcal{O}_k$, then

$$\begin{aligned}
|\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \circ y = o_k^a\}| &= \left|\left\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x^{a^{-1}} \circ y^{a^{-1}} = o_k\right\}\right| \\
&= \left|\left\{(x, y) \in \mathcal{O}_i^{a^{-1}} \times \mathcal{O}_j^{a^{-1}} \mid x \circ y = o_k\right\}\right| \\
&= |\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \circ y = o_k\}| \\
&= \alpha^{\circ}_{ijk}.
\end{aligned}$$

In a finite lattice, the join over all elements is called the *one element*, and the meet over all lattice elements is called *zero element*:

$$1_{\mathcal{L}} := \bigvee_{x \in \mathcal{L}} x, \qquad 0_{\mathcal{L}} := \bigwedge_{x \in \mathcal{L}} x.$$

A lattice $(\mathcal{L}, \vee, \wedge)$ gives rise to two different semigroups $(\mathcal{L}, \vee)$ and $(\mathcal{L}, \wedge)$. The following lemma collects some properties of lattice actions which are in fact actions on these two semigroups:

4.1.4 Lemma *(Plesken [23]) The group A acts on a finite lattice $(\mathcal{L}, \vee, \wedge)$ as a lattice action. Then:*

(i) Any two elements of the same A-orbit are incomparable (i. e. the orbits form anti-chains).

(ii) $0_{\mathcal{L}}$ *and* $1_{\mathcal{L}}$ *are A-orbits of themselves.*

(iii) The orbits of A on $\mathcal{L}$ *form a poset with respect to the ordering*

$$\mathcal{O} \prec \mathcal{O}' :\Longleftrightarrow \exists x \in \mathcal{O}, \exists y \in \mathcal{O}' : x \leq y.$$

We can number the orbits as $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ *in such a way that* $\mathcal{O}_i \prec \mathcal{O}_j$ *implies* $i \leq j$. *Such a numbering is called* topological numbering. *In this numbering,* $\mathcal{O}_1 = \{0_{\mathcal{L}}\}$ *and* $\mathcal{O}_\ell = \{1_{\mathcal{L}}\}$.

(iv) Put $\alpha^{\vee}_{i,j} := \alpha^{\vee}_{ijj}$ *and* $\alpha^{\wedge}_{i,j} := \alpha^{\wedge}_{jii}$ *for* $i, j \leq \ell$. *Then*

$$\alpha^{\vee}_{i,j} = |\{x \in \mathcal{O}_i \mid x \leq o_j\}|$$

and

$$\alpha^{\wedge}_{i,j} = |\{x \in \mathcal{O}_j \mid x \geq o_i\}|.$$

(v) We define $(\ell \times \ell)$*-matrices* $\mathcal{P}(A)^{\vee} = (\alpha^{\vee}_{i,j})$ *and* $\mathcal{P}(A)^{\wedge} = (\alpha^{\wedge}_{i,j})$ *which we call* Plesken matrices. *Let the orbits be sorted topolgically. Then* $\mathcal{P}^{\vee}$ *and* $\mathcal{P}^{\wedge}$ *are upper triangular matrices whose diagonal elements are all one. Moreover,*

$$\begin{aligned} \alpha^{\vee}_{1,j} &= 1, & \alpha^{\wedge}_{1,j} &= |\mathcal{O}_j|, \\ \alpha^{\vee}_{i,\ell} &= |\mathcal{O}_i|, & \alpha^{\wedge}_{i,\ell} &= 1 \end{aligned}$$

for all $0 \leq n, m \leq r$.

(vi) We have

$$\alpha^{\vee}_{i,j} \cdot |\mathcal{O}_j| = |\mathcal{O}_i| \cdot \alpha^{\wedge}_{i,j}$$

for all $1 \leq i, j \leq \ell$. In terms of matrices, this is equivalent to

$$\mathcal{P}(A)^{\vee} \cdot \mathcal{D} = \mathcal{D} \cdot \mathcal{P}(A)^{\wedge},$$

where $\mathcal{D} = \mathrm{diag}(|\mathcal{O}_1|, \ldots, |\mathcal{O}_\ell|)$. In particular,

$$\mathcal{P}(A)^{\wedge} = \mathcal{D}^{-1} \cdot \mathcal{P}(A)^{\vee} \cdot \mathcal{D}.$$

Proof:

(i) Assume z and $z^a = w$ are two different elements of the same A-orbit on $\mathcal{L}$ for some $a \in A$. Assume $z \leq w$ (otherwise, if $w \leq z$ we have $z^{a^{-1}} \geq z$, i. e. we can consider the elements z and $w := z^{a^{-1}}$ and get back to the first case). As $\mathcal{L}$ is finite, $A/\ker(A)$ is a subgroup of the finite group $\mathrm{Sym}_{\mathcal{L}}$, so it is finite, too. Thus there is an integer s with $a^s \in \ker(A)$. Then

$$z \leq z^a \Rightarrow z^a \leq z^{a^2} \Rightarrow \ldots \Rightarrow z^{a^{s-1}} \leq z^{a^s} = z,$$

so $z = z^a = z^{a^2} = \ldots$ contrary to the assumption.

(ii) We have

$$0_{\mathcal{L}}^a = \left(\bigwedge_{x \in \mathcal{L}} x\right)^a = \bigwedge_{x \in \mathcal{L}} x^a = \bigwedge_{x \in \mathcal{L}} x = 0_{\mathcal{L}},$$
$$1_{\mathcal{L}}^a = \left(\bigvee_{x \in \mathcal{L}} x\right)^a = \bigvee_{x \in \mathcal{L}} x^a = \bigvee_{x \in \mathcal{L}} x = 1_{\mathcal{L}}$$

for all $a \in A$ and thus $0_{\mathcal{L}}^A = 0_{\mathcal{L}}$ and $1_{\mathcal{L}}^A = 1_{\mathcal{L}}$.

(iii) (PO1) is clearly satisfied as $x \leq x$ for any element $x \in \mathcal{O}_i$ and thus, $\mathcal{O}_i \prec \mathcal{O}_i$. Assume $\mathcal{O}_i \prec \mathcal{O}_j$ and $\mathcal{O}_j \prec \mathcal{O}_i$ for $1 \leq i, j \leq \ell$. Then there exist $x, x' \in \mathcal{O}_i$ and $y, y' \in \mathcal{O}_j$ with $x \leq y$ and $y' \leq x'$. By transitivity of A on $\mathcal{O}_j$, there exists an $a \in A$ such that $y'^a = y$. Then

$$x \leq y = y'^a \leq x'^a \in \mathcal{O}_i$$

implies $x \leq x'^a$ which by (i) is possible only if $x = x'^a$. But then, $y = x$ and $i = j$ which is (PO2).

In order to show (PO3), let $\mathcal{O}_i \prec \mathcal{O}_j \prec \mathcal{O}_k$ for some $1 \leq i, j, k \leq \ell$. Thus $x \leq y$ and $y' \leq z$ for some $x \in \mathcal{O}_i$, $y, y' \in \mathcal{O}_j$ and some $z \in \mathcal{O}_k$. Then, for some $a \in A$, $y'^a = y$ and

$$x \leq y = y'^a \leq z^a$$

and thus $x \leq z^a$ which implies $\mathcal{O}_i \prec \mathcal{O}_k$.

In order to prove that the elements of the poset can be ordered such that $\mathcal{O}_i \prec \mathcal{O}_j$ implies $i \leq j$ we make use of a graph theoretical argument: We can turn the set of orbits into a directed graph $\mathcal{G}$ which has one vertex for every group orbit. Let V_i be the vertex associated with the orbit $\mathcal{O}_i$. Let there be an edge from V_i to V_j if $\mathcal{O}_i \prec \mathcal{O}_j$ hold in the poset. We write $V_i \mapsto V_j$ if there is an edge from V_i to V_j. The graph $\mathcal{G}$ is acyclic: If there were a cycle $V_{i_1} \mapsto V_{i_2} \mapsto \ldots \mapsto V_{i_r} = V_{i_1}$ then for any $1 < j < r$: $\mathcal{O}_{i_1} \prec \mathcal{O}_{i_j} \prec \mathcal{O}_{i_1}$ which by (PO2) means $\mathcal{O}_{i_j} = \mathcal{O}_{i_1}$. Thus the cycle ist trivial. Now, by a graph theoretic argument (see, for example Manber [21, Section 7.4]) any finite directed acyclic graph can be ordered topologically, i. e. such that $V_i \mapsto V_j$ implies $i \leq j$. Taking the same ordering for the orbits of the group, we find an ordering with the stated property. Note that in a lattice $\mathcal{L}$, all elements lie above $0_{\mathcal{L}}$ and all elements lie below $1_{\mathcal{L}}$. Thus, in any topological ordering $\mathcal{O}_1 = \{0_{\mathcal{L}}\}$ and $\mathcal{O}_\ell = \{1_{\mathcal{L}}\}$.

(iv) An equation $x \vee y = z$ with $x \in \mathcal{O}_i$ and $y, z \in \mathcal{O}_j$ is possible only for $y = z$. Thus,

$$\begin{aligned} \alpha^{\vee}_{i,j} = \alpha^{\vee}_{ijj} &= |\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \vee y = o_j\}| \\ &= |\{x \in \mathcal{O}_i \mid x \vee o_j = o_j\}| \\ &= |\{x \in \mathcal{O}_i \mid x \leq o_j\}| \end{aligned}$$

and

$$\begin{aligned}\alpha^{\wedge}_{i,j} = \alpha^{\wedge}_{jii} &= |\{(x, y) \in \mathcal{O}_j \times \mathcal{O}_i \mid x \wedge y = o_i\}| \\ &= |\{x \in \mathcal{O}_j \mid x \wedge o_i = o_i\}| \\ &= |\{x \in \mathcal{O}_j \mid x \geq o_i\}|.\end{aligned}$$

(v) Let the orbits $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ be sorted topologically. Assume $\alpha^{\vee}_{i,j} \neq 0$ for some $i > j$. Then there exist $x \in \mathcal{O}_i$ and $z \in \mathcal{O}_j$ with $x \leq z$. The topological ordering of orbits implies $i \leq j$, contrary to the assumption. Thus $\mathcal{P}(A)^{\vee}$ is an upper triangular matrix. Moreover,

$$\alpha^{\vee}_{i,i} = |\{x \in \mathcal{O}_i \mid x \leq o_i\}| = |\{o_i\}| = 1,$$

according to (i). The properties of $\mathcal{P}(A)^{\wedge}$ are proved similarly. For $1 \leq i, j \leq \ell$,

$$\begin{aligned}\alpha^{\vee}_{1,j} &= |\{x \in \{0_{\mathcal{L}}\} \mid x \leq o_j\}| = 1, \\ \alpha^{\vee}_{i,\ell} &= |\{x \in \mathcal{O}_i \mid x \leq 1_{\mathcal{L}}\}| = |\mathcal{O}_i|, \\ \alpha^{\wedge}_{i,j} &= |\{x \in \mathcal{O}_j \mid 0_{\mathcal{L}} \leq x\}| = |\mathcal{O}_j|, \\ \alpha^{\wedge}_{i,\ell} &= |\{x \in \{1_{\mathcal{L}}\} \mid o_i \leq x\}| = 1.\end{aligned}$$

(vi) Consider the bipartite graph $\mathcal{G}_{ij}$ whose vertices are the two classes of elements of the orbits $\mathcal{O}_i$ and $\mathcal{O}_j$. An element $x \in \mathcal{O}_i$ is joined by an edge to another element $y \in \mathcal{O}_j$ if $x \leq y$ holds in the lattice. Double counting the edges of the graph $\mathcal{G}_{ij}$ gives

$$\begin{aligned}\#\,\text{edges} &= \sum_{x \in \mathcal{O}_i} |\{y \in \mathcal{O}_j \mid x \leq y\}| = \sum_{x \in \mathcal{O}_i} \alpha^{\wedge}_{i,j} = |\mathcal{O}_i| \cdot \alpha^{\wedge}_{i,j} \\ &= \sum_{y \in \mathcal{O}_j} |\{x \in \mathcal{O}_i \mid x \leq y\}| = \sum_{y \in \mathcal{O}_j} \alpha^{\vee}_{i,j} = |\mathcal{O}_j| \cdot \alpha^{\vee}_{i,j}.\end{aligned}$$

□

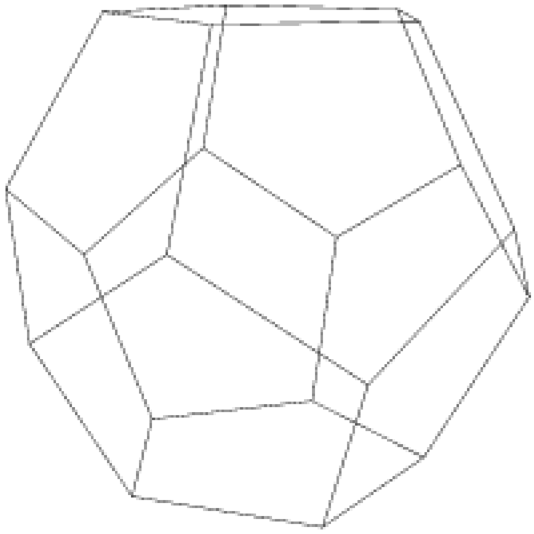


Figure 4.1: The Dodecahedron

4.1.5 Example Take the Dodecahedron (Figure 4.1) and let the sets of vertices, edges and faces be the elements of a lattice $(\mathfrak{D}ode, \subseteq)$. The lattice is defined by inclusion, so an edge is contained in a face if the edge is one of the faces bounding edges. We need two more elements to let this set really become a lattice: the empty set is contained in all elements, and the Dodecahedron itself contains all elements. The Dodecahedron has 20 vertices, 30 edges and 12 faces. Let the group of rotations of the Dodecahedron act on this lattice. This group, isomorphic to Alt_5, is transitive on vertices, edges and faces. So, we have five orbits $\mathcal{O}_{0,1}$, $\mathcal{O}_{1,1}$, $\mathcal{O}_{2,1}$, $\mathcal{O}_{3,1}$, $\mathcal{O}_{4,1}$, corresponding to the elements $\emptyset$, the vertices, the edges, the faces and the Dodecahedron itself. Note that exactly two vertices are contained in an edge, that every face has 5 vertices and that the Dodecahedron has 20 vertices. Moreover, every face contains 5 edges and there are altogether 30 edges. The

Dodecahedron has 12 faces. This yields

$$\mathscr{P}^{\vee}(\mathfrak{D}ode) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 5 & 20 \\ 0 & 0 & 1 & 5 & 30 \\ 0 & 0 & 0 & 1 & 12 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.3}$$

By Lemma 4.1.4 (vi), with

$$\mathscr{D} = \mathrm{diag}(|\mathcal{O}_{0,1}|, \ldots, |\mathcal{O}_{4,1}|) = \mathrm{diag}(1, 20, 30, 12, 1),$$

$$\mathscr{P}^{\wedge}(\mathfrak{D}ode) = \mathscr{D}^{-1} \cdot \mathscr{P}^{\vee}(\mathfrak{D}ode) \cdot \mathscr{D} = \begin{pmatrix} 1 & 20 & 30 & 12 & 1 \\ 0 & 1 & 3 & 3 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.4}$$

$\diamond$

4.2 The Plesken Ring

Let the group A act on the finite semigroup $(M, \circ)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ be the orbits of A on M with representatives $o_i \in \mathcal{O}_i$. For $1 \le i, j, k \le \ell$, let α°_{ijk} be the number defined in (4.2). Plesken defines the following ring:

4.2.1 Definition The $(M, \circ, A)$-ring is a ring with $\mathbb{Z}$-basis $b_1, \ldots, b_\ell$ such that

$$b_i \circ b_j = \sum_{k=1}^{\ell} \alpha^{\circ}_{ijk} b_k \quad \text{for } 1 \le i, j \le \ell.$$

Note that the $(M, \circ, A)$-ring comes together with a distinguished $\mathbb{Z}$-basis. By definition, this ring is unique up to isomorphism. However, it is not at all clear that this ring really exists. This is the first result of Plesken in [23]:

4.2.2 Theorem *The $(M, \circ, A)$-ring exists.*

Proof: Let $(\mathbb{Z}[M], \circ)$ be the semigroup ring of $(M, \circ)$ over $\mathbb{Z}$. We have an embeding $\iota : \mathfrak{P}(M) \hookrightarrow \mathbb{Z}[M],\ X \mapsto \iota(X) := \sum_{m \in X} 1 \cdot m$. We can extend the action of A on M to an action on $(\mathbb{Z}[M], \circ)$ by putting

$$\left(\sum_{m \in M} x_m m\right)^a := \sum_{m \in M} x_m m^a$$

for $a \in A$, $x_m \in \mathbb{Z}$.

Let $(\mathbb{Z}[M]_A, \circ)$ be the subring of A-fixed elements in $(\mathbb{Z}[M], \circ)$, i. e.

$$\mathbb{Z}[M]_A = \{u \in \mathbb{Z}[M] \mid \forall a \in A : \ u^a = u\}.$$

Let $u = \sum_{m \in M} x_m m \in \mathbb{Z}[M]_A$ with $x_m \in \mathbb{Z}$ for all $m \in M$. By definition,

$$\sum_{m \in M} x_m m = u = u^a = \sum_{m \in M} x_m m^a = \sum_{m \in M} x_{m^{a^{-1}}} m,$$

which implies $x_m = x_{m^{a^{-1}}}$ for all $a \in A$. Thus, the coefficients of the elements $u \in \mathbb{Z}[M]_A$ are constant on the orbits of A. On the other hand, all orbit sums

$$b_i := \iota(\mathcal{O}_i) = \sum_{m \in \mathcal{O}_i} m$$

lie in $(\mathbb{Z}[M]_A, \circ)$ which shows that

$$\mathbb{Z}[M]_A = \langle b_i \mid i = 1, \ldots, \ell \rangle_{\mathbb{Z}}.$$

We have

$$\begin{aligned} b_i \circ b_j &= \left(\sum_{x \in \mathcal{O}_i} x\right) \circ \left(\sum_{y \in \mathcal{O}_j} y\right) \\ &= \sum_{z \in M} \sum_{\substack{x \in \mathcal{O}_i, y \in \mathcal{O}_j \\ x \circ y = z}} z \end{aligned}$$

$$= \sum_{k=1}^{\ell} \sum_{z \in \mathcal{O}_k} \underbrace{|\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \circ y = z\}|}_{\alpha^{\circ}_{ijk}} z$$

$$= \sum_{k=1}^{\ell} \alpha^{\circ}_{ijk} b_k,$$

using the fact that the number α°_{ijk} is independent of the choice of the element $z \in \mathcal{O}_k$. □

We call the ring defined in 4.2.1 *Plesken ring.*

We consider the case when $M = \mathcal{L}$ is a lattice. Then $\mathcal{L}$ admits two semigroups $(\mathcal{L}, \vee)$ and $(\mathcal{L}, \wedge)$. Plesken proves that the $(\mathcal{L}, \vee, A)$- and $(\mathcal{L}, \wedge, A)$-rings are in this case isomorphic to a free $\mathbb{Z}$-module with ℓ generators equipped with an additional multiplication which corresponds to the multiplication in the Plesken ring. This multiplication is the Hadamard product of vectors, i. e. the componentwise multiplication of the entries of the vectors. We donote the Haramard product by the symbol $\odot$.

4.2.3 Theorem *(Plesken [23]) The group A acts on the finite lattice $(\mathcal{L}, \vee, \wedge)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ be the orbits of A on $\mathcal{L}$. Let $o_i \in \mathcal{O}_i$ be representatives of the orbits for $1 \le i \le \ell$. Assume that the orbits are sorted topologically as in Lemma 4.1.4. Let $\alpha^{\vee}_{ijk}$ and $\alpha^{\wedge}_{ijk}$ be the structure constants of the $(\mathcal{L}, \vee, A)$- and $(\mathcal{L}, \wedge, A)$-rings $R^{\vee}$ and $R^{\wedge}$, respectively, with $\mathbb{Z}$-bases $(b^{\vee}_1, \ldots, b^{\vee}_\ell)$ and $(b^{\wedge}_1, \ldots, b^{\wedge}_\ell)$. Then:*

(i) The $(\mathcal{L}, \vee, A)$-ring $R^{\vee}$ is isomorphic to $(\mathbb{Z}^\ell, \odot, +)$. The map

$$\varphi^{\vee} : \begin{cases} R^{\vee} & \to \quad (\mathbb{Z}^\ell, \odot, +) \\ b^{\vee}_i & \mapsto \quad \mathfrak{b}^{\vee}_i := (\alpha^{\vee}_{i,1}, \ldots, \alpha^{\vee}_{i,\ell}) \end{cases}$$

with $\alpha^{\vee}_{i,j} = |\{x \in \mathcal{O}_i \mid x \le o_j\}| = \alpha^{\vee}_{ijj}$ for $1 \le i, j \le \ell$ is an isomorphism of rings. $\varphi^{\vee}$ is understood to be the $\mathbb{Z}$-linear extension of the given mapping. In particular,

$$\mathfrak{b}^{\vee}_i \odot \mathfrak{b}^{\vee}_j = \sum_{k=1}^{\ell} \alpha^{\vee}_{ijk} \mathfrak{b}^{\vee}_k .$$

(ii) The $(\mathcal{L}, \wedge, A)$-ring $R^{\wedge}$ is isomorphic to $(\mathbb{Z}^{\ell}, \odot, +)$. The map

$$\varphi^{\wedge} : \left\{ \begin{array}{lcl} R^{\wedge} & \to & (\mathbb{Z}^{\ell}, \odot, +) \\ b_j^{\wedge} & \mapsto & \mathfrak{b}_j^{\wedge} := \begin{pmatrix} \alpha_{1,j}^{\wedge} \\ \vdots \\ \alpha_{\ell,j}^{\wedge} \end{pmatrix} \end{array} \right.$$

with $\alpha_{i,j}^{\wedge} = |\{y \in \mathcal{O}_j \mid y \geq o_i\}| = \alpha_{jii}^{\wedge}$ for $1 \leq i, j \leq \ell$ is an isomorphism of rings. $\varphi^{\wedge}$ is understood to be the $\mathbb{Z}$-linear extension of the given mapping. In particular,

$$\mathfrak{b}_i^{\wedge} \odot \mathfrak{b}_j^{\wedge} = \sum_{k=1}^{\ell} \alpha_{ijk}^{\wedge} \mathfrak{b}_k^{\wedge}.$$

Proof: We only show the first part of the theorem, the second part follows by a similar argument. We verify that $\varphi^{\vee}$ is a homomorphism of rings. By definition, it is a homomorphism of the additive groups. Let us compute the l-th component of $\mathfrak{b}_i^{\vee} \odot \mathfrak{b}_j^{\vee}$ in $\mathbb{Z}^{\ell}$:

$$\begin{aligned} \alpha_{i,l}^{\vee} \cdot \alpha_{j,l}^{\vee} &= |\{x \in \mathcal{O}_i \mid x \leq o_l\}| \cdot |\{y \in \mathcal{O}_j \mid y \leq o_l\}| \\ &= |\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid (x \vee y) \leq o_l\}| \\ &= \sum_{\substack{w \in \mathcal{L} \\ w \leq o_l}} |\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \vee y = w\}| \\ &= \sum_{k=1}^{\ell} \sum_{\substack{w \in \mathcal{O}_k \\ w \leq o_l}} \underbrace{|\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid x \vee y = w\}|}_{=\alpha_{ijk}^{\vee}} \\ &= \sum_{k=1}^{\ell} \alpha_{ijk}^{\vee} \cdot \sum_{\substack{w \in \mathcal{O}_k \\ w \leq o_l}} 1 \\ &= \sum_{k=1}^{\ell} \alpha_{ijk}^{\vee} \cdot \alpha_{k,l}^{\vee}. \end{aligned}$$

Thus we get

$$
\begin{aligned}
\varphi^\vee(b_i^\vee) \odot \varphi^\vee(b_j^\vee) &= \mathfrak{b}_i^\vee \odot \mathfrak{b}_j^\vee \\
&= (\dots, \alpha_{i,l}^\vee, \dots) \odot (\dots, \alpha_{j,l}^\vee, \dots) \\
&= (\dots, \alpha_{i,l}^\vee \cdot \alpha_{j,l}^\vee, \dots) \\
&= (\dots, \sum_{k=1}^{\ell} \alpha_{ijk}^\vee \cdot \alpha_{k,l}^\vee, \dots) \\
&= \sum_{k=1}^{\ell} \alpha_{ijk}^\vee \cdot (\dots, \alpha_{k,l}^\vee, \dots) \\
&= \sum_{k=1}^{\ell} \alpha_{ijk}^\vee \cdot \mathfrak{b}_k^\vee \\
&= \sum_{k=1}^{\ell} \alpha_{ijk}^\vee \cdot \varphi^\vee(b_k^\vee) \\
&= \varphi^\vee\Big(\sum_{k=1}^{\ell} \alpha_{ijk}^\vee \cdot b_k^\vee \Big) \\
&= \varphi^\vee(b_i^\vee \vee b_j^\vee).
\end{aligned}
$$

Note that

$$
\mathcal{P}(A)^\vee = \left(\begin{array}{c} \mathfrak{b}_1^\vee \\ \hline \vdots \\ \hline \mathfrak{b}_\ell^\vee \end{array} \right) = \begin{pmatrix} \alpha_{1,1}^\vee & \dots & \alpha_{1,\ell}^\vee \\ \vdots & & \vdots \\ \alpha_{\ell,1}^\vee & \dots & \alpha_{\ell,\ell}^\vee \end{pmatrix} \tag{4.5}
$$

and

$$
\mathcal{P}(A)^\wedge = \left(\mathfrak{b}_1^\wedge \,\Big|\, \cdots \,\Big|\, \mathfrak{b}_\ell^\wedge \right) = \begin{pmatrix} \alpha_{1,1}^\wedge & \dots & \alpha_{1,\ell}^\wedge \\ \vdots & & \vdots \\ \alpha_{\ell,1}^\wedge & \dots & \alpha_{\ell,\ell}^\wedge \end{pmatrix}. \tag{4.6}
$$

By Lemma 4.1.4 (v), $\mathcal{P}(A)^\vee$ is an upper triangular matrix whose diagonal elements are all one. In particular, it is invertible over $\mathbb{Z}$. The given homomorphism

$\varphi^\vee$ thus is surjective and injective, proving that the rings $R^\vee$ and $\mathbb{Z}^\ell$ are isomorphic. □

4.2.4 Example In the lattice $(\mathfrak{D}ode, \subseteq)$ (cf. Example 4.1.5), the Plesken rings $(\mathfrak{D}ode, \vee, \mathrm{Alt}_5)$ and $(\mathfrak{D}ode, \wedge, \mathrm{Alt}_5)$ have five basis elements $b_0^\vee, \ldots, b_4^\vee$ and $b_0^\wedge, \ldots, b_4^\wedge$. Under the maps $\varphi^\vee$ and $\varphi^\wedge$ of Theorem 4.2.3, these correspond to the five rows of the matrix $\mathcal{P}^\vee(\mathfrak{D}ode)$ and to the five columns of the matrix $\mathcal{P}^\wedge(\mathfrak{D}ode)$ of (4.4). In the Plesken ring we compute the product $b_2^\wedge \wedge b_3^\wedge$. According to Theorem 4.2.3, we get

$$\mathfrak{b}_2^\wedge \odot \mathfrak{b}_3^\wedge = \begin{pmatrix} 30 \\ 3 \\ 1 \\ 0 \\ 0 \end{pmatrix} \odot \begin{pmatrix} 12 \\ 3 \\ 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 360 \\ 9 \\ 2 \\ 0 \\ 0 \end{pmatrix} = 240 \cdot \mathfrak{b}_0^\wedge + 3 \cdot \mathfrak{b}_1^\wedge + 2 \cdot \mathfrak{b}_2^\wedge,$$

which shows, for example, that one can obtain every vertex three times as the intersection of an edge and a face. ◇

4.3 Groups Acting on Ranked Lattices

Let $(\mathcal{L}, \vee, \wedge)$ be a lattice. A *rank function* for $\mathcal{L}$ is a mapping $\mathrm{rk} : \mathcal{L} \to \mathbb{N},\ x \mapsto \mathrm{rk}(x)$ satisfying

$$x < y \Rightarrow \mathrm{rk}(x) < \mathrm{rk}(y) \tag{4.7}$$

for all $x, y \in \mathcal{L}$. Here, $\leq$ is the ordering on $\mathcal{L}$ induced by the lattice as defined in (4.1). A ranked lattice $(\mathcal{L}, \vee, \wedge, \mathrm{rk})$ is a lattice admitting a rank function rk. The condition (4.7) implies for complete lattices

$$\min_{x \in \mathcal{L}} \mathrm{rk}(x) = \mathrm{rk}(0_{\mathcal{L}}) \text{ and } \max_{x \in \mathcal{L}} \mathrm{rk}(x) = \mathrm{rk}(1_{\mathcal{L}}).$$

In case that a group A acts on a complete ranked lattice $\mathcal{L}$, we require

$$\mathrm{rk}(x^a) = \mathrm{rk}(x)$$

for all $x \in \mathcal{L}$ and all $a \in A$. Here are some examples for group actions on ranked lattices.

4.3.1 Examples

(i) Let G be a finite group, $\mathcal{L}(G)$ be its *lattice of subgroups*. The ordering of the groups in the lattice is the usual relation of inclusion. The supremum of two groups U and V is the group which is generated by all elements of U and all elements of V, i. e. $U \vee V =\leq U, V\rangle$. The infimum of two groups U and V is the intersection, i. e. $U \wedge V := U \cap V$. A rank function can be obtained in the following way: Let U be a subgroup of G of order $\prod_{i=1}^{r} p_i^{n_i}$. Put $\mathrm{rk}(U) := \sum_{i=1}^{r} n_i$. Any group $A \leq \mathrm{Aut}(G)$ acts on the lattice of subgroups. Often one considers the action of G itself by conjugation. So, an element $g \in G$ maps $U \in \mathcal{L}(G)$ to U^g. Then $|U^g| = |U| = \prod_{i=1}^{r} p_i^{n_i}$ implies $\mathrm{rk}(U^g) = \mathrm{rk}(U) = \sum_{i=1}^{r} n_i$. Another possible rank funktion is $\mathrm{rk}(U) := |U|$.

(ii) Let $\mathcal{V}$ be a finite set. Consider the *lattice of subsets* $(\mathfrak{P}(\mathcal{V}), \cup, \cap)$. The ordering is given by the usual relation of inclusion for subsets. The supremum and infimum of two sets is the union and antersection of the sets, respectively. A rank function is $\mathrm{rk} : \mathfrak{P}(\mathcal{V}) \to \mathbb{N},\ X \mapsto |X|$. Any group $A \leq \mathrm{Sym}_{\mathcal{V}}$ acts on this lattice by

$$A \times \mathfrak{P}(\mathcal{V}) \to \mathfrak{P}(\mathcal{V}) :\ (a, X) \mapsto X^a.$$

Then $\mathrm{rk}(X^a) = |X^a| = |X| = \mathrm{rk}(X)$.

◇

A rank function induces *layers* on the lattice. The i-th layer consists of the elements of rank i:

$$L^{(i)}(\mathcal{L}) := \{x \in \mathcal{L} \mid \mathrm{rk}(x) = i\}.$$

For the rest of this section, let $\mathcal{L}$ be a *finite* (and thus complete) ranked lattice with a group A acting on it.

We need to extend our terminology for the orbits of A on $\mathcal{L}$. Put $0 = \mathrm{rk}(0_{\mathcal{L}})$ and $r = \mathrm{rk}(1_{\mathcal{L}})$. Then, for $0 \leq i \leq r$, let $\mathcal{O}_{i,1}, \dots, \mathcal{O}_{i,\ell_i}$ be the set of orbits of A on $L^{(i)}(\mathcal{L})$. F"ur $1 \leq j \leq \ell_i$, let $o_{i,j} \in \mathcal{O}_{i,j}$ be representatives of the orbits. Then, for $1 \leq i, j, k \leq \ell$ and $u \leq \ell_i$, $v \leq \ell_j$ and $w \leq \ell_k$ we put

$$\alpha_{u,v,w}^{(i,j,k)^\vee} := |\{(x, y) \in \mathcal{O}_{i,u} \times \mathcal{O}_{j,v} \mid x \vee y = o_{k,w}\}|, \tag{4.8}$$

$$\alpha_{u,v,w}^{(i,j,k)^\wedge} := |\{(x, y) \in \mathcal{O}_{i,u} \times \mathcal{O}_{j,v} \mid x \wedge y = o_{k,w}\}|, \tag{4.9}$$

and

$$\alpha_{u,v}^{(i,j)^\vee} := \alpha_{u,v,v}^{(i,j,j)^\vee} = |\{x \in \mathcal{O}_{i,u} \mid x \leq o_{j,v}\}|, \tag{4.10}$$

$$\alpha_{u,v}^{(i,j)^\wedge} := \alpha_{v,u,u}^{(j,i,i)^\wedge} = |\{x \in \mathcal{O}_{j,v} \mid x \geq o_{i,u}\}|. \tag{4.11}$$

For $1 \leq m, n \leq r$, we have $(\ell_m \times \ell_n)$-matrices

$$\mathcal{P}_{m,n}(A)^\vee := (\alpha_{i,j}^{(m,n)^\vee})_{i,j},$$

$$\mathcal{P}_{m,n}(A)^\wedge := (\alpha_{i,j}^{(m,n)^\wedge})_{i,j}.$$

Putting these matrices together, we get block matrices

$$\mathcal{P}(A)^\vee := (\mathcal{P}_{m,n}(A)^\vee)_{m,n},$$

$$\mathcal{P}(A)^\wedge := (\mathcal{P}_{m,n}(A)^\wedge)_{m,n}.$$

Up to a possible reordering of rows and columns, these matrices coincide with those defined in Lemma 4.1.4. Let us collect some properties of these matrices:

4,3,2 Lemma *Let the group A act on the ranked finite lattice $(\mathcal{L}, \vee, \wedge, \mathrm{rk})$. Let $0 = \mathrm{rk}(0_{\mathcal{L}})$ and $r = \mathrm{rk}(1_{\mathcal{L}})$.*

(i) The $L^{(i)}(\mathcal{L})$ are anti-chains for all $i \leq r$.

(ii) $\ell_0 = \ell_r = 1$ and $\mathcal{O}_{0,1} = \{o_{0,1}\}$ with $o_{0,1} = 0_{\mathcal{L}}$ and $\mathcal{O}_{r,1} = \{o_{r,1}\}$ with $o_{r,1} = 1_{\mathcal{L}}$.

(iii) Let $\mathfrak{b}^{\vee}_{i,j}$ be the j-th row of the i-th row of block matrices $\mathcal{P}_{i,\cdot}(A)^{\vee}$. Let $\mathfrak{b}^{\wedge}_{i,j}$ be the j-th column of the i-th column of block matrices $\mathcal{P}_{\cdot,i}(A)^{\vee}$. Then

$$\mathcal{P}(A)^{\vee} = \left(\begin{array}{c} \mathfrak{b}^{\vee}_{0,1} \\ \vdots \\ \hline \mathfrak{b}^{\vee}_{i,1} \\ \vdots \\ \mathfrak{b}^{\vee}_{i,\ell_i} \\ \hline \vdots \\ \mathfrak{b}^{\vee}_{r,\ell_r} \end{array}\right)$$

and

$$\mathcal{P}(A)^{\wedge} = \left(\begin{array}{c|c|c} \mathfrak{b}^{\wedge}_{0,1} \dots & \mathfrak{b}^{\wedge}_{i,1} \dots \mathfrak{b}^{\wedge}_{i,\ell_i} & \dots \mathfrak{b}^{\wedge}_{r,\ell_r} \end{array}\right).$$

For $0 \leq i,\, j \leq r$, $u \leq \ell_i$ and $v \leq \ell_j$ we have

$$\mathfrak{b}^{\vee}_{i,u} \odot \mathfrak{b}^{\vee}_{j,v} = \sum_{k=0}^{r} \sum_{w=1}^{\ell_k} a^{(i,j,k)^{\vee}}_{u,v,w} \mathfrak{b}^{\vee}_{k,w},$$

$$\mathfrak{b}^{\wedge}_{i,u} \odot \mathfrak{b}^{\wedge}_{j,v} = \sum_{k=0}^{r} \sum_{w=1}^{\ell_k} a^{(i,j,k)^{\wedge}}_{u,v,w} \mathfrak{b}^{\wedge}_{k,w}.$$

(iv) Let $0 \leq n, m \leq r$. Then

$$\mathcal{P}_{0,n}(A)^{\vee} = \underline{1}_{1\times\ell_n}, \qquad \mathcal{P}_{0,n}(A)^{\wedge} = (|\mathcal{O}_{n,1}|, \dots, |\mathcal{O}_{n,\ell_n}|),$$
$$\mathcal{P}_{m,r}(A)^{\vee} = (|\mathcal{O}_{m,1}|, \dots, |\mathcal{O}_{m,\ell_m}|)^{\top}, \; \mathcal{P}_{m,r}(A)^{\wedge} = \underline{1}_{\ell_m\times 1}.$$

(v) *Let* $0 \leq n < m \leq r$. *Then*

$$\mathcal{P}_{m,n}(A)^{\vee} = \mathcal{P}_{m,n}(A)^{\wedge} = \underline{0}_{\ell_m \times \ell_n},$$
$$\mathcal{P}_{m,m}(A)^{\vee} = \mathcal{P}_{m,m}(A)^{\wedge} = I_{\ell_m}.$$

(vi) *Let* $\mathcal{D}_i = \operatorname{diag}(|\mathcal{O}_{i,1}|, \ldots, |\mathcal{O}_{i,\ell_i}|)$ *for* $0 \leq i \leq r$. *Then*

$$\mathcal{P}_{m,n}(A)^{\wedge} = \mathcal{D}_m^{-1} \cdot \mathcal{P}_{m,n}(A)^{\vee} \cdot \mathcal{D}_n$$

for $0 \leq m, n \leq r$. *Equivalently*

$$\mathcal{P}(A)^{\wedge} = \mathcal{D}^{-1} \cdot \mathcal{P}(A)^{\vee} \cdot \mathcal{D}$$

with $\mathcal{D} := \operatorname{diag}(\mathcal{D}_1, \ldots, \mathcal{D}_r)$.

Proof:

(i) Let $x, y \in L^{(i)}(\mathcal{L})$. Then $x < y \Rightarrow \operatorname{rk}(x) < \operatorname{rk}(y)$ contradicting $\operatorname{rk}(x) = \operatorname{rk}(y) = i$.

(ii) By the properties of the rank function, $L^{(0)} = \{0_{\mathcal{L}}\}$ and $L^{(r)} = \{1_{\mathcal{L}}\}$. By Lemma 4.1.4 (ii), these two elements form two orbits of length 1, so $\mathcal{O}_{0,1} = \{0_{\mathcal{L}}\}$ and $\mathcal{O}_{r,1} = \{1_{\mathcal{L}}\}$.

(iii) Rewriting the result of Theorem 4.2.3 with the new indices, we get the two equations from the Plesken ring structure.

(iv) Let $j \leq \ell_n$ and $i \leq \ell_m$. Then,

$$\begin{aligned}
\alpha_{1,j}^{(0,n)^{\vee}} &= |\{x \in \{0_{\mathcal{L}}\} \mid x \leq o_{n,j}\}| = 1 \\
&\Rightarrow \quad \mathcal{P}_{0,n}(A)^{\vee} = \underline{1}_{1 \times \ell_n}, \\
\alpha_{i,1}^{(m,r)^{\vee}} &= |\{x \in \mathcal{O}_{m,i} \mid x \leq 1_{\mathcal{L}}\}| = |\mathcal{O}_{m,i}| \\
&\Rightarrow \quad \mathcal{P}_{m,r}(A)^{\vee} = (|\mathcal{O}_{m,1}|, \ldots, |\mathcal{O}_{m,\ell_m}|)^{\top},
\end{aligned}$$

$$\begin{aligned}
\alpha_{1,j}^{(0,n)\wedge} &= |\{x \in \mathcal{O}_{n,j} \mid x \geq 0_{\mathfrak{L}}\}| = |\mathcal{O}_{n,j}| \\
&\Rightarrow \quad \mathcal{P}_{0,n}(A)^{\wedge} = (|\mathcal{O}_{n,1}|, \ldots, |\mathcal{O}_{n,\ell_n}|), \\
\alpha_{i,1}^{(m,r)\wedge} &= |\{x \in \{1_{\mathfrak{L}}\} \mid x \geq o_{m,i}\}| = 1 \\
&\Rightarrow \quad \mathcal{P}_{m,r}(A)^{\wedge} = \underline{1}_{\ell_m \times 1}.
\end{aligned}$$

(v) If $n < m$, no element of $L^{(m)}$ is less than an element of $L^{(n)}$. So

$$\mathcal{P}_{m,n}(A)^{\vee} = \mathcal{P}_{m,n}(A)^{\wedge} = \underline{0}_{\ell_m \times \ell_n}.$$

The equation

$$\mathcal{P}_{m,m}(A)^{\vee} = \mathcal{P}_{m,m}(A)^{\wedge} = I_{\ell_m}$$

follows from (i) and from

$$\alpha_{i,i}^{(m,m)\vee} = \alpha_{i,i}^{(m,m)\wedge} = 1.$$

(vi) Lemma 4.1.4 (iv) applied to the $\alpha_{i,j}^{(m,n)\vee}$ and $\alpha_{i,j}^{(m,n)\wedge}$ yields

$$\alpha_{i,j}^{(m,n)\vee} \cdot |\mathcal{O}_{n,j}| = |\mathcal{O}_{m,i}| \cdot \alpha_{i,j}^{(m,n)\wedge}.$$

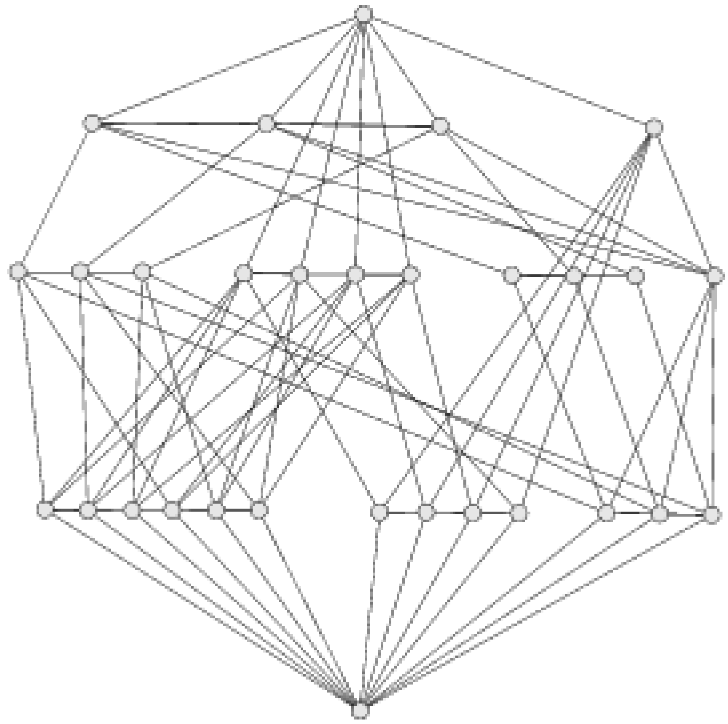
In matrix terms, this is

$$\mathcal{P}_{m,n}(A)^{\vee} \cdot \mathcal{D}_n = \mathcal{D}_m \cdot \mathcal{P}_{m,n}(A)^{\wedge}$$

which implies the statement.

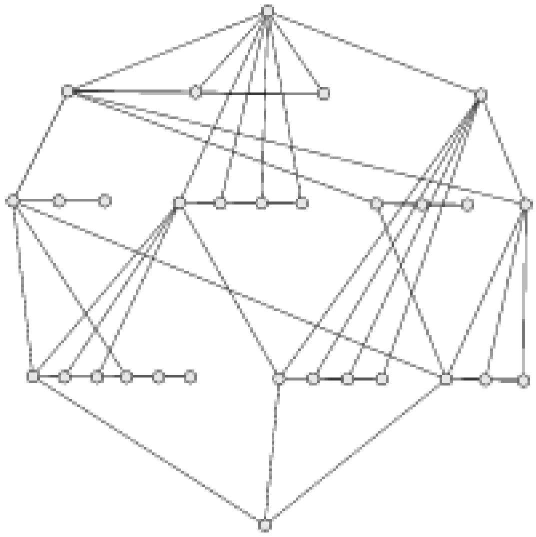
□

4.3.3 Example Consider $\mathfrak{L}(\mathrm{Sym}_4)$, the subgroup lattice of Sym_4 (cf. Figure 4.2, below a table of the conjugacy classes of subgroups). Figure 4.3 shows the $\vee$-picture of the lattice and the Plesken matrix $\mathcal{P}^{\vee}(\mathrm{Sym}_4)$. In the bottom line, the $\wedge$-picture and the Plesken matrix $\mathcal{P}^{\wedge}(\mathrm{Sym}_4)$ are shown. In both matrices, the block decomposition by the rank function is indicated by horizontal and vertical lines within the matrices. ◇

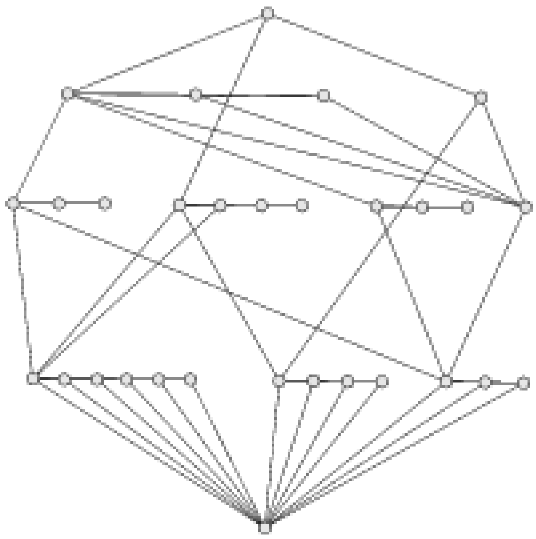


orbit $\mathcal{O}_{i,j}$	representative $O_{i,j}$	type	$\lvert\mathcal{O}_{i,j}\rvert$	$\lvert O_{i,j}\rvert$	rk $O_{i,j}$
$\mathcal{O}_{0,1}$	$\langle id\rangle$		1	1	0
$\mathcal{O}_{1,1}$	$\langle(1,2)\rangle$	$\simeq \mathbb{Z}_2$	6	2	1
$\mathcal{O}_{1,2}$	$\langle(1,2,3)\rangle$	$\simeq \mathbb{Z}_3$	4	3	1
$\mathcal{O}_{1,3}$	$\langle(1,2)(3,4)\rangle$	$\simeq \mathbb{Z}_2$	3	2	1
$\mathcal{O}_{2,1}$	$\langle(1,2),(3,4)\rangle$	$\simeq \mathbb{Z}_2\times\mathbb{Z}_2$	3	4	2
$\mathcal{O}_{2,2}$	$\langle(1,2,3),(1,2)\rangle$	$\simeq \mathrm{Sym}_3$	4	6	2
$\mathcal{O}_{2,3}$	$\langle(1,2,3,4)\rangle$	$\simeq \mathbb{Z}_4$	3	4	2
$\mathcal{O}_{2,4}$	$\langle(1,2)(3,4),(1,3)(2,4)\rangle$	$\simeq V_4$	1	4	2
$\mathcal{O}_{3,1}$	$\langle(1,2,3,4),(1,3)\rangle$	$\simeq D_4$	3	8	3
$\mathcal{O}_{3,2}$	$\langle(1,2)(3,4)(1,2,3)\rangle$	$\simeq \mathrm{Alt}_4$	1	12	3
$\mathcal{O}_{4,1}$	$\langle(1,2,3,4),(1,2)\rangle$	$\simeq \mathrm{Sym}_4$	1	24	4

Figure 4.2: The Subgroup Lattice of Sym_4



$$\left(\begin{array}{c|ccc|cccc|cc|c}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline
 & 1 & 0 & 0 & 2 & 3 & 0 & 0 & 2 & 0 & 6 \\
 & & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 4 & 4 \\
 & & & 1 & 1 & 0 & 1 & 3 & 3 & 3 & 3 \\ \hline
 & & & & 1 & 0 & 0 & 0 & 1 & 0 & 3 \\
 & & & & & 1 & 0 & 0 & 0 & 0 & 4 \\
 & & & & & & 1 & 0 & 1 & 0 & 3 \\
 & & & & & & & 1 & 1 & 1 & 1 \\ \hline
 & & & & & & & & 1 & 0 & 3 \\
 & & & & & & & & & 1 & 1 \\ \hline
 & & & & & & & & & & 1
\end{array}\right)$$



$$\left(\begin{array}{c|ccc|cccc|cc|c}
1 & 6 & 4 & 3 & 3 & 4 & 3 & 1 & 3 & 1 & 1 \\ \hline
 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 1 \\
 & & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
 & & & 1 & 1 & 0 & 1 & 1 & 3 & 1 & 1 \\ \hline
 & & & & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & & & & & 1 & 0 & 0 & 0 & 0 & 1 \\
 & & & & & & 1 & 0 & 1 & 0 & 1 \\
 & & & & & & & 1 & 3 & 1 & 1 \\ \hline
 & & & & & & & & 1 & 0 & 1 \\
 & & & & & & & & & 1 & 1 \\ \hline
 & & & & & & & & & & 1
\end{array}\right)$$

Figure 4.3: The Subgroup Lattice of Sym_4, $\vee$ picture, Plesken Matrix $\mathcal{P}^{\vee}(\mathrm{Sym}_4)$ (top), $\wedge$ picture, Plesken Matrix $\mathcal{P}^{\wedge}(\mathrm{Sym}_4)$ (bottom)

4.4 Acting on the Subset Lattice

In this section, we consider the action of groups on subset lattices. We obtain stronger results which are based on the structure of the subset lattice.

4.4.1 Lemma *Let $\mathcal{V}$ be a v-element set and let A be a permutation group on $\mathcal{V}$. We consider the induced action of A on the lattice $(\mathfrak{P}(\mathcal{V}), \cup, \cap, |\cdot|)$ with rank function $\mathfrak{P}(\mathcal{V}) \to \{0, \ldots, v\}$, $X \mapsto |X|$. Let $L^{(i)}(\mathfrak{P}(\mathcal{V})) = \binom{\mathcal{V}}{i}$ be the i-th layer of the lattice. For $0 \leq i \leq v$, let $\mathcal{O}_{i,1}, \ldots, \mathcal{O}_{i,\ell_i}$ be the orbits of A on $L^{(i)}(\mathfrak{P}(\mathcal{V}))$ with representatives $O_{i,j} \in \mathcal{O}_{i,j}$.*

(i) For $0 \leq m \leq n \leq v$, the following is true:

$$\underline{1}_{1\times\ell_m} \cdot \mathcal{P}_{m,n}(A)^{\cup} = \binom{n}{m} \cdot \underline{1}_{1\times\ell_n},$$
$$\mathcal{P}_{m,n}(A)^{\cap} \cdot \underline{1}_{\ell_n\times 1} = \binom{v-m}{n-m} \cdot \underline{1}_{\ell_m\times 1}.$$

(ii) For $0 \leq m \leq h \leq n \leq v$, the following recursion formulae are satisfied:

$$\binom{n-m}{h-m} \cdot \mathcal{P}_{m,n}(A)^{\cup} = \mathcal{P}_{m,h}(A)^{\cup} \cdot \mathcal{P}_{h,n}(A)^{\cup},$$
$$\binom{n-m}{h-m} \cdot \mathcal{P}_{m,n}(A)^{\cap} = \mathcal{P}_{m,h}(A)^{\cap} \cdot \mathcal{P}_{h,n}(A)^{\cap}.$$

(iii) The inverse matrices are

$$\left(\mathcal{P}(A)^{\cup}\right)^{-1} = \left((-1)^{m+n}\mathcal{P}_{m,n}(A)^{\cup}\right)_{m,n},$$
$$\left(\mathcal{P}(A)^{\cap}\right)^{-1} = \left((-1)^{m+n}\mathcal{P}_{m,n}(A)^{\cap}\right)_{m,n}.$$

(iv) If $A = \mathrm{Sym}_{\mathcal{V}}$, then $\ell_0 = \ell_1 = \ldots = \ell_v = 1$, i. e. $\mathrm{Sym}_{\mathcal{V}}$ is transitive on i-subsets for all $i \leq v$. We have $\mathcal{P}_{m,n}(\mathrm{Sym}_{\mathcal{V}})^{\cup} = \binom{n}{m}$ and thus

$$\mathcal{P}(\mathrm{Sym}_{\mathcal{V}})^{\cup} = (\mathcal{P}_{m,n}(\mathrm{Sym}_{\mathcal{V}})^{\cup}) = \mathcal{B}_{[0,\ldots,v],[0,\ldots,v]}$$

and $\mathcal{P}_{m,n}(\mathrm{Sym}_{\mathcal{V}})^{\cap} = \binom{v-m}{n-m}$ and

$$\mathcal{P}(\mathrm{Sym}_{\mathcal{V}})^{\cap} = (\mathcal{P}_{m,n}(\mathrm{Sym}_{\mathcal{V}})^{\cap}).$$

Proof:

(i) We show that the elements in every column of $\mathcal{P}_{m,n}(A)^{\cup}$ sum up to $\binom{n}{m}$: For $j \leq \ell_n$, we compute

$$\begin{aligned}
\sum_{i=1}^{\ell_m} \alpha_{i,j}^{(m,n)^{\cup}} &= \sum_{i=1}^{\ell_m} |\{X \in \mathcal{O}_{m,i} \mid X \subseteq O_{n,j}\}| \\
&= |\{X \in \underbrace{\bigcup_{i=1}^{\ell_m} \mathcal{O}_{m,i}}_{=L^{(m)}(\mathfrak{P}(\mathcal{V}))=\binom{\mathcal{V}}{m}} \mid X \subseteq O_{n,j}\}| \\
&= \binom{n}{m}.
\end{aligned}$$

We show that the sum of all elements of as row of $\mathcal{P}_{m,n}(A)^{\cap}$ is equal to $\binom{v-m}{n-m}$: For all $i \leq \ell_m$ we have

$$\begin{aligned}
\sum_{j=1}^{\ell_n} \alpha_{i,j}^{(m,n)^{\cap}} &= \sum_{j=1}^{\ell_n} |\{Y \in \mathcal{O}_{n,j} \mid O_{m,i} \subseteq Y\}| \\
&= |\{Y \in \underbrace{\bigcup_{j=1}^{\ell_n} \mathcal{O}_{n,j}}_{=L^{(n)}(\mathfrak{P}(\mathcal{V}))=\binom{\mathcal{V}}{n}} \mid O_{m,i} \subseteq Y\}| \\
&= \binom{v-m}{n-m}.
\end{aligned}$$

(ii) (Following Schmalz [25, Satz 2.3.5, page 40]) We first prove the correctness of the second equation involving the $\mathcal{P}_{m,n}(A)^{\cap}$. On both sides of the equation, we have matrices whose rows and columns are indexed in the same order by m- and n-orbits of A. Let $x_{i,k}$ be the (i,k)-th entry of the left matrix, and let $x'_{i,k}$ be the (i,k)-th entry of the matrix on the right hand side. By definition, $x_{i,k} = \binom{n-m}{h-m}\alpha_{i,k}^{(m,n)^{\cap}}$. We compute the corresponding matrix entry on the right hand side:

$$\begin{aligned}
x'_{i,k} &= \sum_{j=1}^{\ell_h} \alpha_{i,j}^{(m,h)^\cap} \cdot \alpha_{j,k}^{(h,n)^\cap} \\
&\overset{(4.11)}{=} \sum_{j=1}^{\ell_h} \alpha_{j,i,i}^{(h,m,m)^\cap} \cdot \alpha_{k,j,j}^{(n,k,h)^\cap} \\
&= \sum_{j=1}^{\ell_h} |\{H \in \mathcal{O}_{h,j} \mid O_{m,i} \subseteq H\}| \cdot |\{N \in \mathcal{O}_{n,k} \mid O_{h,j} \subseteq N\}| \\
&= \sum_{j=1}^{\ell_h} \left|\left\{(H,N) \in \mathcal{O}_{h,j} \times \mathcal{O}_{n,k} \mid O_{m,i} \subseteq H \subseteq N\right\}\right| \\
&= \left|\left\{(H,N) \in \underbrace{\bigcup_{j=1}^{\ell_h} \mathcal{O}_{h,j}}_{=L^{(h)}(\mathfrak{P}(\mathcal{V}))=\binom{\mathcal{V}}{h}} \times \mathcal{O}_{n,k} \mid O_{m,i} \subseteq H \subseteq N\right\}\right| \\
&= \sum_{\substack{N \in \mathcal{O}_{n,k} \\ O_{m,i} \subseteq N}} \left|\left\{H \in \binom{\mathcal{V}}{h} \mid O_{m,i} \subseteq H \subseteq N\right\}\right| \\
&= \sum_{\substack{N \in \mathcal{O}_{n,k} \\ O_{m,i} \subseteq N}} \binom{n-m}{h-m} \\
&= \binom{n-m}{h-m} \cdot \alpha_{i,k}^{(m,n)^\cap} \\
&= x_{i,k}.
\end{aligned}$$

Using 4.3.2 (vi), we get the recursion formula for the $\mathcal{P}_{m,n}(A)^\cup$:

$$\begin{aligned}
\binom{n-m}{h-m}\mathcal{P}_{m,n}(A)^\cup &= \mathcal{D}_m \cdot \binom{n-m}{h-m} \cdot \mathcal{P}_{m,n}(A)^\cap \cdot \mathcal{D}_n^{-1} \\
&= \mathcal{D}_m \cdot \mathcal{P}_{m,h}(A)^\cap \cdot \mathcal{D}_h^{-1} \cdot \mathcal{D}_h \cdot \mathcal{P}_{h,n}(A)^\cap \cdot \mathcal{D}_n^{-1} \\
&= \mathcal{P}_{m,h}(A)^\cup \cdot \mathcal{P}_{h,n}(A)^\cup.
\end{aligned}$$

(iii) We prove by induction on the difference $n-m$ that the inverse matrix $\left(\mathscr{P}(A)^{\cup}\right)^{-1}$ has the form $\left((-1)^{m+n}\cdot\mathscr{P}(A)^{\cup}_{m,n}\right)$. Recall from Lemma 4.3.2 (iii) that $\mathscr{P}(A)^{\cup}=\left(\mathscr{P}(A)^{\cup}_{m,n}\right)$ is an upper triangular blockmatrix. This means that $\mathscr{P}(A)^{\cup}_{m,n}=\underline{0}$ for $n<m$. The diagonal matrices are identity matrices: $\mathscr{P}(A)^{\cup}_{m,m}=I_{\ell_m}$. Denote the blocks of the inverse matrix by $\left(\mathscr{P}(A)^{\cup}\right)^{-1}=(\mathscr{P}'_{m,n})$. Then $\mathscr{P}'_{m,n}=\underline{0}$ for $n<m$ and $\mathscr{P}'_{m,m}=I_{\ell_m}$, i. e. the formula is valid for $n=m$ or $n-m=0$. Now let us determine $\mathscr{P}'_{m,n}$ for $n-m>0$. As $\left(\mathscr{P}(A)^{\cup}\right)\cdot\left(\mathscr{P}(A)^{\cup}\right)^{-1}=I$ we get in the m-th row and n-th column of the block matrices

$$
\begin{aligned}
&& \sum_{h=0}^{v}\mathscr{P}_{m,h}(A)^{\cup}\cdot\mathscr{P}'_{h,n}&=\underline{0}_{\ell_m\times\ell_n}\\
\Longleftrightarrow && \sum_{h=m}^{n}\mathscr{P}_{m,h}(A)^{\cup}\cdot\mathscr{P}'_{h,n}&=\underline{0}_{\ell_m\times\ell_n}\\
\Longleftrightarrow && I_{\ell_m}\cdot\mathscr{P}'_{m,n}+\sum_{h=m+1}^{n}\mathscr{P}_{m,h}(A)^{\cup}\cdot\mathscr{P}'_{h,n}&=\underline{0}_{\ell_m\times\ell_n}\\
\Longleftrightarrow && \mathscr{P}'_{m,n}&=-\sum_{h=m+1}^{n}\mathscr{P}_{m,h}(A)^{\cup}\cdot\mathscr{P}'_{h,n}
\end{aligned}
$$

and by induction

$$
\begin{aligned}
\mathscr{P}'_{m,n}&=-\sum_{h=m+1}^{n}\mathscr{P}_{m,h}(A)^{\cup}\cdot\mathscr{P}'_{h,n}\\
&=-\sum_{h=m+1}^{n}(-1)^{h+n}\cdot\mathscr{P}_{m,h}(A)^{\cup}\cdot\mathscr{P}_{h,n}(A)^{\cup}\\
&=(-1)^{n+1}\sum_{h=m+1}^{n}(-1)^{h}\cdot\binom{n-m}{h-m}\cdot\mathscr{P}_{m,n}(A)^{\cup}\\
&=(-1)^{n+1}\left(\sum_{h=1}^{n-m}(-1)^{m+h}\cdot\binom{n-m}{h}\right)\cdot\mathscr{P}_{m,n}(A)^{\cup}
\end{aligned}
$$

$$= (-1)^{n+m+1}\Bigg(\underbrace{\left[\sum_{h=0}^{n-m}(-1)^h \cdot \binom{n-m}{h}\right]}_{=0} - 1\Bigg) \cdot \mathcal{P}_{m,n}(A)^{\cup}$$
$$= (-1)^{n+m} \cdot \mathcal{P}_{m,n}(A)^{\cup}.$$

The proof for $\left(\mathcal{P}(A)^{\cap}\right)^{-1}$ is done in a similar way.

(iv) The group $A := \mathrm{Sym}_{\mathcal{V}}$ is transitive on i-subsets of $\mathcal{V}$. Thus, each layer holds exactly one orbit $\mathcal{O}_{m,1}$ with a representing set $O_{m,1}$. Then

$$\alpha_{1,1}^{(m,n)\cup} = \left|\left\{X \in \mathcal{O}_{m,1} = \binom{\mathcal{V}}{m} \mid X \subseteq O_{n,1}\right\}\right| = \binom{n}{m},$$

and

$$\alpha_{1,1}^{(m,n)\cap} = \left|\left\{Y \in \mathcal{O}_{n,1} = \binom{\mathcal{V}}{n} \mid O_{m,1} \subseteq Y\right\}\right| = \binom{v-m}{n-m}.$$

□

Note that the statements (iii) and (v) together yield another proof of Lemma 1.3.20, i. e. of

$$\mathcal{B}^{-1} = (b'_{i,j}) \quad \text{with} \quad b'_{i,j} = (-1)^{i+j}\binom{j}{i}.$$

There is a close connection between the Plesken matrices for the action on subset lattices and the results of Section 3.1. By definition, the matrix $\mathcal{M}_{t,k}^{A}$ of Theorem 3.1.1 is just one of the matrices in the block matrix decomposition of $\mathcal{P}(A)^{\cap}$:

4.4.2 Lemma *The group A acts on the set $\mathcal{V} = \{1, \ldots, v\}$. Let $0 \le t \le k \le v$ be integers. Then*

$$\mathcal{M}_{t,k}^{A} = \mathcal{P}_{t,k}(A)^{\cap},$$

if both matrices are indexed in the same order by the t- and k-orbits of A.

Chapter 5

Classification of Designs

In this chapter we shall describe a way to compute the intersection numbers of a design with a known group of automorphisms. The method uses knowledge about the orbits of that group A on subsets. Background of this method is the Plesken ring of the action of the group A on the subset lattice.

5.1 The Computation of Intersection Numbers

We consider global intersection numbers $\alpha^{(s)}(\mathcal{D})$ and $\alpha^{[s]}(\mathcal{D})$ of a design $\mathcal{D}$ for integral $s \geq 1$. We put

$$\mathcal{A}^{(s)} := \left(\alpha^{(1)}(\mathcal{D})^{\top}\middle| \ \dots \ \middle|\alpha^{(s)}(\mathcal{D})^{\top}\right)$$

and

$$\mathcal{A}^{[s]} := \left(\alpha^{[1]}(\mathcal{D})^{\top}\middle| \ \dots \ \middle|\alpha^{[s]}(\mathcal{D})^{\top}\right)$$

and call these matrices the *matrices of global intersection numbers.*

Let $\mathcal{V} = \{1, \dots, v\}$ be the set of points and let $A \leq \mathrm{Sym}_{\mathcal{V}}$ be the prescribed automorphism group. We assume that we know the orbits of the group A on i-subsets of $\mathcal{V}$ for $i \leq k$. Let $\mathcal{O}_{i,1}, \dots, \mathcal{O}_{i,\ell_i}$ be the i-orbits of A for $0 \leq i \leq k$.

let $O_{i,j} \in \mathcal{O}_{i,j}$ be representatives of these orbits. For $0 \leq m, n \leq k$ we have the Plesken matrices $\mathcal{P}_{m,n}(A)^{\cap}$, which together form one big $((k+1) \times (k+1))$-block matrix $\mathcal{P}(A)^{\cap} = (\mathcal{P}_{m,n}(A)^{\cap})$. Let $\mathfrak{b}_{i,j}^{\cap}$ be the columns of this matrix. The Plesken ring $(\mathcal{P}(A)^{\cap}, \odot, +)$ is generated by the columns of thie matrix over $\mathbb{Z}$.

We make use of the weight function $\kappa : \mathbb{Z}[\mathfrak{P}(\mathcal{V})] \to \mathcal{W}_v$, introduced in the proof of Theorem 2.3.1, where $\mathcal{W}_v$ is the free $\mathbb{Z}$-module of rank $(v+1)$, generated by the uni vectors $\mathfrak{e}_0, \ldots, \mathfrak{e}_v$. Restricting to the A-fixsubring $\mathbb{Z}[\mathfrak{P}(\mathcal{V})]_A$ we obtain a mapping

$$\kappa : (\mathbb{Z}[\mathfrak{P}(\mathcal{V})]_A, \cap, +) \to \mathcal{W}_v, \sum_{M \subseteq \mathcal{V}} a_M \cdot M \mapsto \sum_{M \subseteq \mathcal{V}} a_M \cdot \mathfrak{e}_{|M|}, \tag{5.1}$$

where all a_M are integers and $\sum_{M \subseteq \mathcal{V}} a_M \cdot M$ is fix under A, which means that the coefficients a_M are constant on the orbits of A.

Let ν be the following weight function from the Plesken ring $(\mathcal{P}(A)^{\cap}, \odot, +)$ to $\mathcal{W}_v$. This mapping ν shall be the distributive $\mathbb{Z}$-linear extension of

$$\nu : (\mathcal{P}(A)^{\cap}, \odot, +) \to \mathcal{W}_v,\ \mathfrak{b}_{i,j}^{\cap} \mapsto |\mathcal{O}_{i,j}| \cdot \mathfrak{e}_i. \tag{5.2}$$

The connection between κ and ν is the following:

5.1.1 Lemma *Let A be a group acting on $\mathcal{V}$, and let $\mathcal{O}_{i,1}, \ldots, \mathcal{O}_{i,\ell_i}$ be the orbits of A on i-subsets. Let $\iota(\mathcal{O}_{i,j}) := \sum_{X \in \mathcal{O}_{i,j}} X$ be the sum of all elements in the orbit $\mathcal{O}_{i,j}$ as an element of the semigroup ring $(\mathbb{Z}[\mathfrak{P}(\mathcal{V})]_A, \cap, +)$. Let $\kappa : (\mathbb{Z}[\mathfrak{P}(\mathcal{V})]_A, +, \cap) \to \mathcal{W}_v$ be the mapping defined in (5.1), and let $(\mathcal{P}(A)^{\cap}, \odot, +)$ be the Plesken ring with weight map $\nu : (\mathcal{P}(A)^{\cap}, \odot, +) \to \mathcal{W}_v$ as defined in (5.2). Then*

$$\kappa = \nu \circ \varphi^{\cap},$$

where $\varphi^{\cap}$ is the map defined in Theorem 4.2.3, sending the j-th orbit sum $\iota(\mathcal{O}_{i,j})$ onto the basis element $\mathfrak{b}_{i,j}^{\cap} := \begin{pmatrix} \mathfrak{b}_0^{\cap} \\ \hline \vdots \\ \hline \mathfrak{b}_v^{\cap} \end{pmatrix}$ *with* $\mathfrak{b}_h^{\cap} = (\alpha_{1,j}^{(h,i)^{\cap}}, \ldots, \alpha_{\ell_h,j}^{(h,i)^{\cap}})^{\top}$ *for* $h = 0, \ldots, v$.

Proof: We verify the stated equaltity for the generators of the ring $(\mathbb{Z}[\mathfrak{P}(\mathcal{V})]_A, \cap, +)$, i. e. for the orbit sums $\iota(\mathcal{O}_{i,j})$:

$$\begin{aligned}\kappa(\iota(\mathcal{O}_{i,j})) &= \kappa\Big(\sum_{B\in\mathcal{O}_{i,j}} B\Big) = \sum_{B\in\mathcal{O}_{i,j}} \mathfrak{e}_{|B|} = |\mathcal{O}_{i,j}|\cdot\mathfrak{e}_i = \nu\left(\mathfrak{b}^{\cap}_{i,j}\right)\\ &= \left(\nu\circ\varphi^{\cap}\right)(\iota(\mathcal{O}_{i,j})).\end{aligned}$$

□

Next comes the main result allowing the computation of global intersection numbers of designs:

5.1.2 Theorem *Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a t-(v,k,λ) design with $A \leq \mathrm{Aut}(\mathcal{D})$. Let $\mathfrak{x}$ be the solution vector of the design, i. e. $\mathcal{B} = \mathcal{B}_{\mathfrak{x}} = \bigcup_{\substack{j=1\\ \mathfrak{x}(j)=1}}^{\ell_k} \mathcal{O}_{k,j}$. Let $\mathfrak{z} = \sum_{\substack{j=1\\ \mathfrak{x}(j)=1}}^{\ell_k} \mathfrak{b}^{\cap}_{k,j}$. We split the vector $\mathfrak{z}$ in the following way:*

$$\mathfrak{z} = \begin{pmatrix} \mathfrak{z}_0 \\ \hline \mathfrak{z}_1 \\ \hline \vdots \\ \hline \mathfrak{z}_k \end{pmatrix} \quad \textit{with} \quad \mathfrak{z}_i = \begin{pmatrix} z_{i,1} \\ z_{i,2} \\ \vdots \\ z_{i,\ell_i} \end{pmatrix}.$$

Let $\mathcal{B}^{-1}_{[0\ldots k],[0\ldots k]}$ be the $((k+1)\times(k+1))$-matrix whose (i,j)-th coefficient is $(-1)^{i+j}\binom{j}{i}$, which by Lemma 1.3.20 is the inverse of the matrix of binomial coefficients. Let $\mathcal{S}_1$ be the $(s\times s)$-matrix of Stirling numbers of the first kind $\mathcal{S}_1 = (\mathcal{S}_1(i,j))$ and let $\mathcal{D} = \mathrm{diag}\big(\frac{1}{1!}, \frac{1}{2!}, \ldots, \frac{1}{s!}\big)$. Then,

$$\mathcal{A}^{[s]} = \mathcal{B}^{-1}_{[0\ldots k],[0\ldots k]} \cdot \mathcal{Z}_s(A, \mathfrak{x}), \tag{5.3}$$

$$\mathcal{A}^{(s)} = \mathcal{A}^{[s]} \cdot \mathcal{S}_1^{\top} \cdot \mathcal{D}, \tag{5.4}$$

$$\mathcal{A}^{(s)} = \mathcal{B}^{-1}_{[0\ldots k],[0\ldots k]} \cdot \mathcal{Z}_s(A, \mathfrak{x}) \cdot \mathcal{S}_1^{\top} \cdot \mathcal{D}. \tag{5.5}$$

with the $((k+1)\times s)$*-matrix*

$$\mathbb{Z}_s(A,\mathfrak{r}) := \left(\begin{array}{ccc} \binom{v}{0}\lambda_0^1 & \cdots & \binom{v}{0}\lambda_0^s \\ \vdots & & \vdots \\ \binom{v}{t}\lambda_t^1 & \cdots & \binom{v}{t}\lambda_t^s \\ \hline \mathcal{P}_{0,t+1}(A)^{\cap}\cdot\odot^1\mathfrak{z}_{t+1} & \cdots & \mathcal{P}_{0,t+1}(A)^{\cap}\cdot\odot^s\mathfrak{z}_{t+1} \\ \vdots & & \vdots \\ \mathcal{P}_{0,k-1}(A)^{\cap}\cdot\odot^1\mathfrak{z}_{k-1} & \cdots & \mathcal{P}_{0,k-1}(A)^{\cap}\cdot\odot^s\mathfrak{z}_{k-1} \\ \hline b & \cdots & b \end{array}\right). \tag{5.6}$$

Proof: Let $\mathcal{O}_{i,j}$ be the j-th orbit of A on i-subsets, for $1\le j\le \ell_i$. Let $\mathcal{P}(A)^{\cap} = \left(\mathcal{P}_{m,n}(A)^{\cap}\right)$ be the Plesken matrix for the action of A on the subset lattice of $\mathcal{V}$ for the layers $0,\dots,k$. Let $\mathfrak{b}_{i,j}^{\cap}$ for $0\le i\le k$ and $1\le j\le \ell_i$ be the column in the Plesken matrix corresponding to the j-th orbit of A on i-subsets.

$$\mathfrak{z}_i = \mathcal{P}_{i,k}(A)^{\cap}\cdot\mathfrak{r}^{\top}. \tag{5.7}$$

In the Plesken ring, we may decompose

$$\odot^s\mathfrak{z} = \sum_{i=0}^{k}\sum_{j=1}^{\ell_i} y_{i,j}^{[s]}\cdot\mathfrak{b}_{i,j}^{\cap} \tag{5.8}$$

with unknown coefficients $y_{i,j}^{[s]}\in\mathbb{Z}$ (in fact, these coefficients are nonnegative as they describe a certain number of orbits). We get a vector

$$\mathfrak{y}^{[s]} = \left(\begin{array}{c} \mathfrak{y}_0^{[s]} \\ \hline \mathfrak{y}_1^{[s]} \\ \hline \vdots \\ \hline \mathfrak{y}_k^{[s]} \end{array}\right) \quad\text{with}\quad \mathfrak{y}_i^{[s]} = \begin{pmatrix} y_{i,1}^{[s]} \\ y_{i,2}^{[s]} \\ \vdots \\ y_{i,\ell_i}^{[s]} \end{pmatrix} \quad\text{for}\quad 0\le i\le k. \tag{5.9}$$

Then

$$\odot^s\mathfrak{z} = \mathcal{P}(A)^{\cap}\cdot\mathfrak{y}^{[s]} \iff \mathfrak{y}^{[s]} = \mathcal{P}(A)^{\cap -1}\cdot\odot^s\mathfrak{z}.$$

By Lemma 4.3.2 (v) and Lemma 4.4.1 (iii), the matrix

$$\mathscr{P}(A)^{\cap -1} = \left((-1)^{i+j}\mathscr{P}_{i,j}(A)^{\cap}\right)$$

is an upper triangular block matrix. Thus, we obtain

$$\mathfrak{y}_i^{[s]} = \sum_{j=i}^{k}(-1)^{i+j}\mathscr{P}_{i,j}(A)^{\cap}\cdot \odot^s \mathfrak{z}_j \tag{5.10}$$

for $i = 0, 1, \ldots, k$. We now compute

$$\begin{aligned}
\alpha^{[s]}(\mathcal{D}) &= \kappa\left(\sum_{(B_{j_1},\ldots,B_{j_s})\in\mathcal{B}^s}\bigcap_{k=1}^{s} B_{j_k}\right)\\
&= \kappa\left(\bigcap^{s}\sum_{j=1}^{b} B_j\right)\\
&= \kappa\left(\bigcap^{s}\sum_{\substack{j=1\\ \mathfrak{p}(j)=1}}^{\ell_k}\sum_{B\in\mathcal{O}_{k,j}} B\right)\\
&= \kappa\left(\bigcap^{s}\sum_{\substack{j=1\\ \mathfrak{p}(j)=1}}^{\ell_k}\iota(\mathcal{O}_{k,j})\right)
\end{aligned}$$

by Lemma 5.1.1, $\kappa = \nu\circ\varphi^{\cap}$, so we get

$$\overset{5.1.1}{=} \quad \nu\left(\left(\bigcap^{s}\sum_{\substack{j=1\\ \mathfrak{p}(j)=1}}^{\ell_k}\iota(\mathcal{O}_{k,j})\right)^{\varphi^{\cap}}\right),$$

which is an element of the A-fixsubring $\mathbb{Z}[\mathfrak{P}(\mathcal{V})]_A$, and by Pleskens Theorem4.2.3 (ii), the ringisomorphism $\varphi^{\cap}$ maps this expression onto

$$\overset{4.2.3\text{ (ii)}}{=} \quad \nu\left(\bigodot^{s}\sum_{\substack{j=1\\ \mathfrak{p}(j)=1}}^{\ell_k}\mathfrak{b}_{k,j}^{\cap}\right)$$

$$
\begin{aligned}
&= \quad \nu\left(\odot^s \mathfrak{z}\right)\\
&\overset{(5.8)}{=} \quad \nu\left(\sum_{i=0}^{k}\sum_{j=1}^{\ell_i} y_{i,j}^{[s]} \cdot \mathfrak{b}_{i,j}^{\cap}\right)\\
&= \quad \sum_{i=0}^{k}\sum_{j=1}^{\ell_i} y_{i,j}^{[s]} \cdot \nu(\mathfrak{b}_{i,j}^{\cap})\\
&\overset{(5.2)}{=} \quad \sum_{i=0}^{k}\left\{\sum_{j=1}^{\ell_i} |\mathcal{O}_{i,j}| \cdot y_{i,j}^{[s]}\right\} \cdot \mathfrak{e}_i .
\end{aligned}
$$

By Lemma 4.3.2 (iv), $\mathcal{P}_{0,i}(A)^{\cap} = (\mathcal{O}_{i,1}, \ldots, \mathcal{O}_{i,\ell_i})$. Using (5.9) we can rewrite the inner sum as a matrix product:

$$
\begin{aligned}
&\overset{\substack{4.3.2\text{ (iv)}\\(5.9)}}{=} \quad \sum_{i=0}^{k} \mathcal{P}_{0,i}(A)^{\cap} \cdot \mathfrak{y}_i^{[s]} \cdot \mathfrak{e}_i\\
&\overset{(5.10)}{=} \quad \sum_{i=0}^{k}\left\{\sum_{j=i}^{k}(-1)^{i+j}\underbrace{\mathcal{P}_{0,i}(A)^{\cap}\cdot\mathcal{P}_{i,j}(A)^{\cap}}_{=\binom{j}{i}\mathcal{P}_{0,j}(A)^{\cap}} \cdot \odot^s \underbrace{\mathfrak{z}_j}_{=\mathcal{P}_{j,k}(A)^{\cap}\cdot\mathfrak{x}^{\top}}\right\}\cdot \mathfrak{e}_i ,
\end{aligned}
$$

and with Lemma 4.4.1 (ii) and Equation (5.7) we obtain

$$
\overset{4.4.1\text{ (ii)}}{=} \quad \sum_{i=0}^{k}\left\{\sum_{j=i}^{k}(-1)^{i+j}\binom{j}{i}\mathcal{P}_{0,j}(A)^{\cap}\cdot\odot^s\left(\mathcal{P}_{j,k}(A)^{\cap}\cdot\mathfrak{x}^{\top}\right)\right\}\cdot\mathfrak{e}_i .
$$

By Lemma 4.4.2, $\mathcal{P}_{j,k}(A)^{\cap} = \mathcal{M}_{j,k}^{A}$ is the Kramer Mesner matrix. As every t-design is also a j-design for all $j \leq t$ we get by Corollary 3.1.4

$$
\begin{aligned}
\overset{\substack{4.4.2\\3.1.4}}{=} \quad & \sum_{i=0}^{k}\Bigg\{\sum_{j=i}^{t}(-1)^{i+j}\binom{j}{i}\mathcal{P}_{0,j}(A)^{\cap}\cdot\odot^s(\lambda_j\cdot\underline{1}_{\ell_j\times 1})\\
&+\sum_{j=t+1}^{k-1}(-1)^{i+j}\binom{j}{i}\mathcal{P}_{0,j}(A)^{\cap}\cdot\odot^s\mathfrak{z}_j
\end{aligned}
$$

$$+ (-1)^{i+k}\binom{k}{i}\mathcal{P}_{0,k}(A)^{\cap} \cdot \odot^{s}\mathfrak{x}^{\top}\Bigg\} \cdot \mathfrak{e}_i,$$

using the fact that by Lemma 4.3.2 (v) $\mathcal{P}_{k,k}(A)^{\cap} = I_{\ell_k}$ is the identity matrix. As $\mathfrak{x}$ is a $\{0, 1\}$-vector we get $\odot^{s}\mathfrak{x}^{\top} = \mathfrak{x}^{\top}$, and thus

$$\overset{\mathfrak{x} \in \{0,1\}^{\ell_k}}{=} \sum_{i=0}^{k}\Bigg\{\sum_{j=i}^{t}(-1)^{i+j}\binom{j}{i}\underbrace{\mathcal{P}_{0,j}(A)^{\cap} \cdot \underline{1}_{\ell_j \times 1}}_{=\binom{v}{j}} \cdot \lambda_j^{s}$$

$$+ \sum_{j=t+1}^{k-1}(-1)^{i+j}\binom{j}{i}\mathcal{P}_{0,j}(A)^{\cap} \cdot \odot^{s}\mathfrak{z}_j$$

$$+ (-1)^{i+k}\binom{k}{i}\underbrace{\mathcal{P}_{0,k}(A)^{\cap} \cdot \mathfrak{x}^{\top}}_{=\lambda_0 = b}\Bigg\} \cdot \mathfrak{e}_i.$$

By Lemma 4.4.1 (i), the row sum of the Plesken matrix is knows. As $\mathcal{P}_{0,j}(A)^{\cap}$ is one-rowed, $\mathcal{P}_{0,j}(A)^{\cap} \cdot \underline{1}_{\ell_j \times 1} = \binom{v}{j}$. Moreover, $\mathcal{P}_{0,k}(A)^{\cap} \cdot \mathfrak{x}^{\top} = \lambda_0 = b$ so by Corollary 3.1.4

$$\overset{4.4.1(\mathrm{i}),\ 3.1.4}{=} \sum_{i=0}^{k}\Bigg\{\sum_{j=i}^{t}(-1)^{i+j}\binom{j}{i}\binom{v}{j} \cdot \lambda_j^{s}$$

$$+ \sum_{j=t+1}^{k-1}(-1)^{i+j}\binom{j}{i}\mathcal{P}_{0,j}(A)^{\cap} \cdot \odot^{s}\mathfrak{z}_j + (-1)^{i+k}\binom{k}{i} \cdot b\Bigg\} \cdot \mathfrak{e}_i.$$

Writing this equation in matrix form, we arrive at

$$\mathcal{A}^{[s]} = \mathcal{B}^{-1}_{[0\ldots k],[0\ldots k]} \cdot \mathcal{Z}_s(A, \mathfrak{x}),$$

where $\mathcal{Z}_s(A, \mathfrak{x})$ is the matrix defined in (5.6). This proves (5.3). Equation (5.4) then follows from Theorem 2.3.1, and both equations together imply (5.5). This finishes the proof. □

Let us apply the result to an example:

5,1,3 Example We shall examine the 5-(24, 8, 1) Witt design which is invariant under M_{24}. The parameters $\lambda_{i,j}$ for $i + j \le t = 5$ are:

$\lambda_{i,j}$	$j = 0,$	1,	2,	3,	4,	5
$i = 0$	759	506	330	210	130	78
1	253	176	120	80	52	
2	77	56	40	28		
3	21	16	12			
4	5	4				
5	1					

Recall that we put $\lambda_i = \lambda_{i,0}$. The values of $\binom{v}{i} = \binom{24}{i}$ for $i = 0, 1, \ldots, 5$ are:

$$(1, 24, 276, 2024, 10626, 42504)\,.$$

We choose $s = 3$ and obtain

$$\begin{aligned}
\mathcal{A}^{(3)} &= \mathcal{B}^{-1}_{[0..8],[0..8]} \cdot Z_3(M_{24}, \mathfrak{x}) \cdot \mathcal{S}1^{\top}_{[1..3],[1..3]} \cdot \mathcal{D} \\
&= \begin{pmatrix}
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
0 & 1 & -2 & 3 & -4 & 5 & -6 & 7 & -8 \\
0 & 0 & 1 & -3 & 6 & -10 & 15 & -21 & 28 \\
0 & 0 & 0 & 1 & -4 & 10 & -20 & 35 & -56 \\
0 & 0 & 0 & 0 & 1 & -5 & 15 & -35 & 70 \\
0 & 0 & 0 & 0 & 0 & 1 & -6 & 21 & -56 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -7 & 28 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -8 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \\
&\quad \cdot Z_3(M_{24}, \mathfrak{x}) \cdot \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} \cdot \operatorname{diag}(\frac{1}{1!}, \frac{1}{2!}, \frac{1}{3!}).
\end{aligned}$$

	$\{\}^{244823040,1}$	$\{1\}^{10200960,24}$	$\{1,2\}^{887040,276}$	$\{1,2,3\}^{120960,2024}$	$\{1,2,3,4\}^{23040,10626}$	$\{1,2,3,4,5\}^{5760,42504}$	$\{1,2,3,4,5,6\}^{2160,113344}$	$\{1,2,3,4,5,8\}^{11520,21252}$	$\{1,2,3,4,5,6,7\}^{720,340032}$	$\{1,2,3,4,5,8,11\}^{40320,6072}$	$\{1,2,3,4,5,6,7,8\}^{384,637560}$	$\{1,2,3,4,5,6,7,17\}^{2520,97152}$	$\{1,2,3,4,5,8,11,13\}^{322560,759}$
$\{\}$	1	24	276	2024	10626	42504	113344	21252	340032	6072	637560	97152	759
$\{1\}$	0	1	23	253	1771	8855	28336	5313	99176	1771	212520	32384	253
$\{1,2\}$	0	0	1	22	231	1540	6160	1155	25872	462	64680	9856	77
$\{1,2,3\}$	0	0	0	1	21	210	1120	210	5880	105	17640	2688	21
$\{1,2,3,4\}$	0	0	0	0	1	20	160	30	1120	20	4200	640	5
$\{1,2,3,4,5\}$	0	0	0	0	0	1	16	3	168	3	840	128	1
$\{1,2,3,4,5,6\}$	0	0	0	0	0	0	1	0	18	0	135	18	0
$\{1,2,3,4,5,8\}$	0	0	0	0	0	0	0	1	16	2	120	32	1
$\{1,2,3,4,5,6,7\}$	0	0	0	0	0	0	0	0	1	0	15	2	0
$\{1,2,3,4,5,8,11\}$	0	0	0	0	0	0	0	0	0	1	0	16	1
$\{1,2,3,4,5,6,7,8\}$	0	0	0	0	0	0	0	0	0	0	1	0	0
$\{1,2,3,4,5,6,7,17\}$	0	0	0	0	0	0	0	0	0	0	0	1	0
$\{1,2,3,4,5,8,11,13\}$	0	0	0	0	0	0	0	0	0	0	0	0	1

Table 5.1: The Plesken Matrix $\mathscr{P}(M_{24})^{\cap}$

Here,

$$Z_3(A, \mathfrak{x}_i) = \left(\begin{array}{ccc} \binom{24}{0}\lambda_0^1 & \cdots & \binom{24}{0}\lambda_0^3 \\ \vdots & & \vdots \\ \binom{24}{5}\lambda_5^1 & \cdots & \binom{24}{5}\lambda_5^3 \\ \hline \mathcal{P}_{0,6}(M_{24})^{\cap} \cdot \odot^1 \mathfrak{z}_6 & \cdots & \mathcal{P}_{0,6}(M_{24})^{\cap} \cdot \odot^3 \mathfrak{z}_6 \\ \mathcal{P}_{0,7}(M_{24})^{\cap} \cdot \odot^1 \mathfrak{z}_7 & \cdots & \mathcal{P}_{0,7}(M_{24})^{\cap} \cdot \odot^3 \mathfrak{z}_7 \\ \hline b & \cdots & b \end{array}\right)$$

$$= \begin{pmatrix} 759 & 576081 & 437.245479 \\ 6072 & 1536216 & 388.662648 \\ 21252 & 1636404 & 126.003108 \\ 42504 & 892584 & 18.744264 \\ 53130 & 265650 & 1.328250 \\ 42504 & 42504 & 42504 \\ \gamma_{6,1}(\mathfrak{x}) & \gamma_{6,2}(\mathfrak{x}) & \gamma_{6,3}(\mathfrak{x}) \\ \gamma_{7,1}(\mathfrak{x}) & \gamma_{7,2}(\mathfrak{x}) & \gamma_{7,3}(\mathfrak{x}) \\ 759 & 759 & 759 \end{pmatrix}$$

with numbers $\gamma_{i,u}(\mathfrak{x}) = \mathcal{P}_{0,i}(M_{24})^{\cap} \cdot \odot^u \mathfrak{z}_i$, depending on the solution vector via $\mathfrak{z} = \sum_{\substack{j=1 \\ \mathfrak{x}(j)=1}}^{\ell_8} \mathfrak{b}_{8,j}^{\cap}$. As $\mathfrak{x} = (0, 0, 1)$, this reduces to $\mathfrak{z} = \mathfrak{b}_{8,3}^{\cap}$, i. e.

$$\mathfrak{z} = (759, 253, 77, 21, 5, 1, 0, 1, 0, 1, 0, 0, 1)^{\top}.$$

Splitting the vector $\mathfrak{z}$ into pieces we get

$$\begin{aligned} \mathfrak{z}_0 &= (759)^{\top}, & \mathfrak{z}_1 &= (253)^{\top}, & \mathfrak{z}_2 &= (77)^{\top}, \\ \mathfrak{z}_3 &= (21)^{\top}, & \mathfrak{z}_4 &= (5)^{\top}, & \mathfrak{z}_5 &= (1)^{\top}, \\ \mathfrak{z}_6 &= (0, 1)^{\top}, & \mathfrak{z}_7 &= (0, 1)^{\top}, & \mathfrak{z}_8 &= (0, 0, 1)^{\top}. \end{aligned}$$

Next we compute

$$\gamma_{6,u}(\mathfrak{x}) = \begin{pmatrix} 113344 & 21252 \end{pmatrix} \cdot \odot^u (0, 1)^{\top} = 21252 \quad \text{for} \quad u = 1, 2, 3,$$

$$\gamma_{7,u}(\mathfrak{x}) = \begin{pmatrix} 340032 & 6072 \end{pmatrix} \cdot \odot^u (0,1)^\top = 6072 \quad \text{for} \quad u = 1,2,3$$

and obtain

$$\mathcal{A}^{(3)} = \begin{pmatrix} 0 & 11385 & 26.179175 \\ 0 & 0 & 31.282944 \\ 0 & 170016 & 12.751200 \\ 0 & 0 & 2266880 \\ 0 & 106260 & 106260 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 759 & 0 & 0 \end{pmatrix}.$$

◇

The result of Theorem 5.1.2 may be seen as an extension of Lemma 2.3.2 The notation shall be as before.

5.1.4 Corollary *Let $\mathcal{D}$ be a t-(v, k, λ) design with prescribed automorphism group A and with solution vector $\mathfrak{x}$. Then for $s \geq 1$:*

$$\mathcal{B}_{[0,\dots,k],[0,\dots,k]} \cdot \mathcal{A}^{(s)} = \mathcal{Z}_s(A, \mathfrak{x}) \cdot \mathcal{S}_1^\top \cdot \mathcal{D}. \tag{5.11}$$

In particular we get the equations of Lemma 2.3.2 back from the first $t + 1$ rows of this linear system.

Proof: (5.11) follows directly from (5.5). In the first $t + 1$ rows we get

$$\mathcal{B}_{[0,\dots,t],[0,\dots,k]} \cdot \mathcal{A}^{(s)} = \operatorname{diag}\Big(\binom{v}{0}, \dots, \binom{v}{t}\Big) \begin{pmatrix} \lambda_0^1 & \dots & \lambda_0^s \\ \vdots & & \vdots \\ \lambda_t^1 & \dots & \lambda_t^s \end{pmatrix} \cdot \mathcal{S}_1^\top \cdot \mathcal{D},$$

using Lemma 1.3.19 (iii) which implies

$$\sum_{k=0}^{s} \lambda_i^k \cdot \mathscr{s}_1(u,k) \cdot \frac{1}{u!} = \frac{1}{u!}[\lambda_i]_u = \binom{\lambda_i}{u},$$

for $i = 0, \ldots, t$ and $u = 1, \ldots, s$ we get:

$$= \operatorname{diag}\left(\binom{v}{0}, \ldots, \binom{v}{t}\right) \cdot \begin{pmatrix} \binom{\lambda_0}{1} & \cdots & \binom{\lambda_0}{s} \\ \vdots & & \vdots \\ \binom{\lambda_t}{1} & \cdots & \binom{\lambda_t}{s} \end{pmatrix}$$

$$= \begin{pmatrix} \binom{v}{0}\binom{\lambda_0}{1} & \cdots & \binom{v}{0}\binom{\lambda_0}{s} \\ \vdots & & \vdots \\ \binom{v}{t}\binom{\lambda_t}{1} & \cdots & \binom{v}{t}\binom{\lambda_t}{s} \end{pmatrix}. \tag{5.12}$$

Reading out the s-th column of (5.12) yields the first statement of Lemma 2.3.2.

□

5.2 Classification of 8-(31, 10, λ) Designs

Let us try to classify the 8-(31, 10, λ) designs from Section 3.2. Recall that we have 138 designs with $\lambda = 93$ and 1658 designs with $\lambda = 100$. The group which we prescribed was $A = \mathrm{PSL}(3, 5)$ on 31 points. We consider the following submatrix of the Plesken matrix $\mathscr{P}(A)^{\cap}$:

	$\ell_8 = 42$	$\ell_9 = 92$	$\ell_{10} = 174$
$\ell_8 = 42$	I_{42}	$\mathscr{P}_{8,9}(A)^{\cap}$	$\mathscr{P}_{8,10}(A)^{\cap}$
$\ell_9 = 92$	$\underline{0}$	I_{92}	$\mathscr{P}_{9,10}(A)^{\cap}$
$\ell_{10} = 174$	$\underline{0}$	$\underline{0}$	I_{174}

The matrix $\mathcal{P}_{8,10}(A)^{\cap}$ has already been displayed in Tables 3.3 and 3.4. We show $\mathcal{P}_{8,9}(A)^{\cap}$ in Table 5.2. Tables 5.3 to 5.5 show $\mathcal{P}_{9,10}(A)^{\cap}$ split into three parts. Recall that we replaced the numbers 10 and higher by small letters $a, b, c, \ldots$.

We first consider the 138 designs with $\lambda = 93$. We label the solutions of the system

$$\mathcal{P}_{8,10}(A)^{\cap} \cdot \mathfrak{x}^{\top} = 93 \cdot \underline{1}_{42\times 1},$$

by $\mathfrak{x}_1, \ldots, \mathfrak{x}_{138}$. The parameters λ_i are:

$$\begin{aligned} \lambda_0 &= 16\,303365, & \lambda_3 &= 435240, & \lambda_6 &= 4650,\\ \lambda_1 &= 5\,259150, & \lambda_4 &= 108810, & \lambda_7 &= 744,\\ \lambda_2 &= 1\,577745, & \lambda_5 &= 24180, & \lambda_8 &= 93. \end{aligned}$$

The values of $\binom{v}{i} = \binom{31}{i}$ for $0 \le i \le 8$ are

$$1, 31, 465, 4495, 31465, 169911, 736281, 2629575, 7\,888725.$$

Acccording to Theorem 5.1.2, Equation (5.5), we compute the matrix of intersection invariants $\mathcal{A}^{(3)}$ in the following way:

$$\mathcal{A}^{(3)} = \mathcal{B}^{-1}_{[0..10],[0...10]} \cdot Z_s(A, \mathfrak{x}_i) \cdot \mathcal{S}1^{\top}_{[1,\ldots,3][1,\ldots,3]} \cdot \operatorname{diag}\Big(\frac{1}{1!}, \frac{1}{2!}, \frac{1}{3!}\Big)$$

$$= \begin{pmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1\\ 0 & 1 & -2 & 3 & -4 & 5 & -6 & 7 & -8 & 9 & -10\\ 0 & 0 & 1 & -3 & 6 & -10 & 15 & -21 & 28 & -36 & 45\\ 0 & 0 & 0 & 1 & -4 & 10 & -20 & 35 & -56 & 84 & -120\\ 0 & 0 & 0 & 0 & 1 & -5 & 15 & -35 & 70 & -126 & 210\\ 0 & 0 & 0 & 0 & 0 & 1 & -6 & 21 & -56 & 126 & -252\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -7 & 28 & -84 & 210\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -8 & 36 & -120\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -9 & 45\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -10\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

```
21k.......................................................................................
.3.k......................................................................................
..3122424212..............................................................................
...1..422211622...........................................................................
.1......8..48..2..........................................................................
2..............1g4........................................................................
..1.....1.......2.1111211121111111........................................................
..1........1....2.2.....2...2.2..222221...................................................
..1.........1...11..11.1.1.1.1.11..1111.12211.............................................
....2............84.............4...........14............................................
.....11...........1111..3.1.11....21..........2111111.....................................
....1.....1.......2.22...........12.............2..22222..................................
........4.............44...........4........1........4...2................................
.......1.1............2.1.111..1.1.1.1.......11.1.1...1...111111..........................
......2..................11.11.....11........121....12..1.1.2...1111......................
.......2..................22..2.1...2.....1.....2..2..2..1.2....2.........................
........2..2............2..2.2.2.2....2..........2.....11......1.1.1......................
.........2....................2212...2....1...2....22....1..22............................
....1.........1......2.2...2......2....2.............2...1...2..2..22.....................
.....1.......1......4..........4.....4.2..................4..........12...................
......1......1..........1...1......11....3.........1.1......211.11..21.111................
........1..12..........1....1.1.....1...11...1..1...11..1..1..1..1.2.21...................
......2...............1........2.....2..4......12......1.....2.1..122.....................
........2...2..............2.......2.....2....2.........12.1...2..1..2.11.................
..........1...1.................2.........1........2....2.22....22.4....2.................
.......1.1.............22..2..1.........22.2........2.....2.....2.....2...................
..........2...........................1....4......4..8.................4..................
............4............................................2.24..2.2....4.21................
..............2...........................4...................4...4.....81................
..................2..2.......................2.32...2...1.................111222..........
...................2..1.2.2.2.....2...............................1.......11.6..12........
....................4............4.........4..........2.................1...2.....1221....
.....................2...2..........2..24...................221.........1...1...1.1...2...
......................1..11.11.....11........1....121.....1..2..1............2.1.2.1.1....
......................1..2......2...2....2.2..1............1..1.2...2.............2...12..
........................1112.1.1.1...1..2.....1.1.........1.....1............111.2..1.11..
..................8....................................2..................4...24........12
...................22.............4.............2..2............211.........1...32......1.
..................1.1..1..1..111.11.1..1............1.....1..1.....1.......1....22.1...2..
................................24....1.........4.2..........................4.2..2......2
..................2222............................1.22.....................4.2.1...1.1..1.
................................4.....1...2........4......4...4....................4......
```

Table 5.2: $\mathscr{P}_{8,9}(\mathrm{PSL}(3,5))^{\cap}$

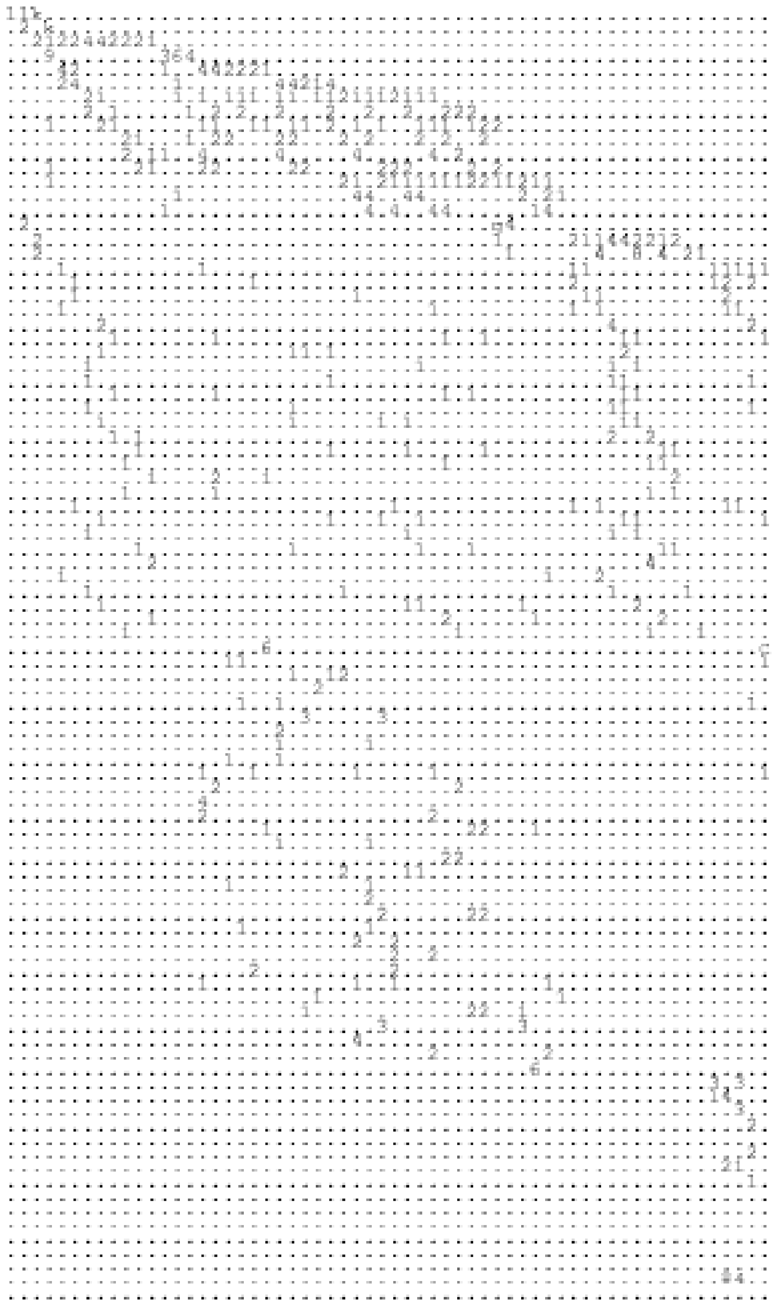


Table 5.3: $\mathscr{P}_{9,10}(\mathrm{PSL}(3,5))^{\cap}$, Left Part

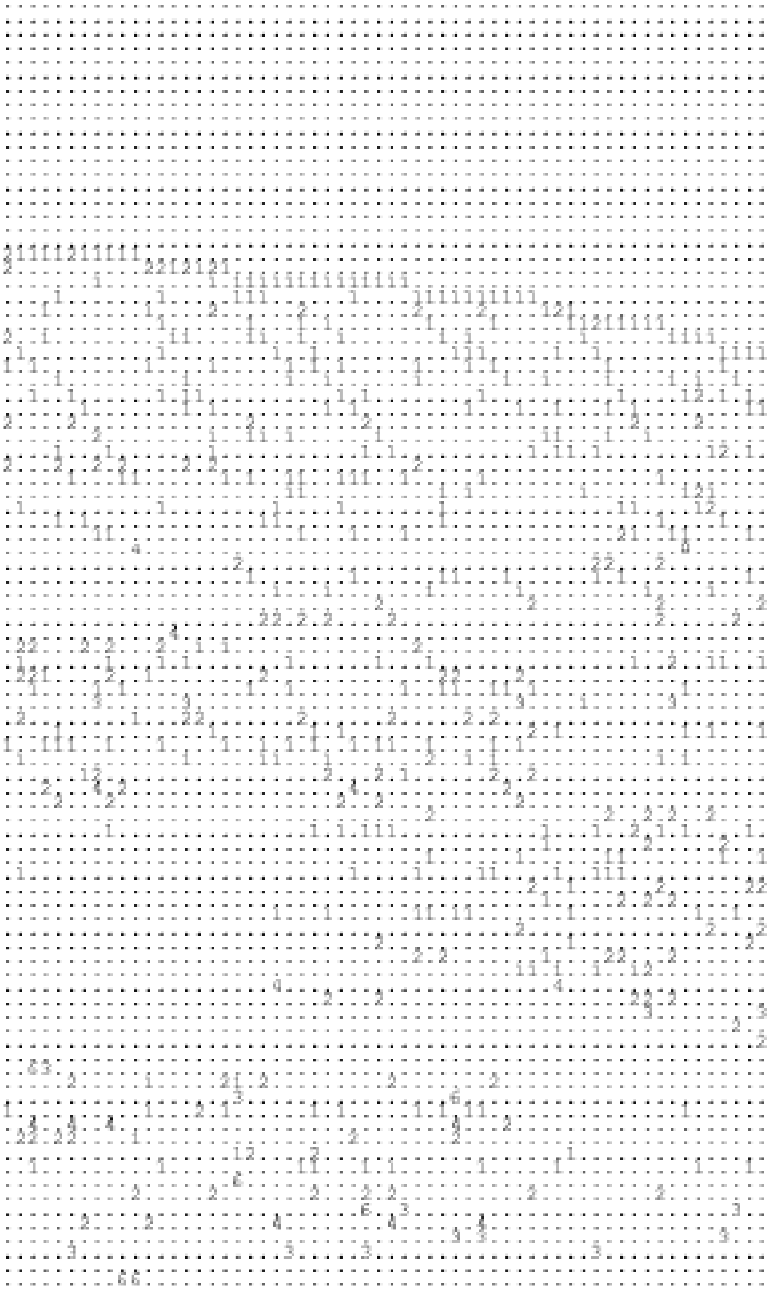


Table 5.4: $\mathscr{P}_{9,10}(\mathrm{PSL}(3,5))^{\cap}$, Middle Part

[illegible]

Table 5.5: $\mathscr{P}_{9,10}(\mathrm{PSL}(3,5))^{\cap}$, Right Part

$$\cdot\, \mathcal{Z}_3(A,\mathfrak{x}_i)\cdot \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{6} \end{pmatrix}.$$

Here, $\mathcal{Z}_3(A,\mathfrak{x}_i)$ is the matrix

$$\mathcal{Z}_3(A,\mathfrak{x}_i) = \begin{pmatrix} \binom{31}{0}\lambda_0^1 & \cdots & \binom{31}{0}\lambda_0^3 \\ \vdots & & \vdots \\ \binom{31}{8}\lambda_8^1 & \cdots & \binom{31}{8}\lambda_8^3 \\ \hline \mathcal{P}_{0,9}(A)^{\cap}\cdot \odot^1\mathfrak{z}_9 & \cdots & \mathcal{P}_{0,9}(A)^{\cap}\cdot \odot^3\mathfrak{z}_9 \\ \hline b & \cdots & b \end{pmatrix}$$

$$= \begin{pmatrix} 16\,303365 & 265\,799710\,323225 & 4333\,429694\,293805\,152125 \\ 163\,033650 & 857\,418420\,397500 & 4509\,292085\,633512\,125000 \\ 733\,651425 & 1157\,514867\,536625 & 1826\,263294\,681572\,410625 \\ 1956\,403800 & 851\,505189\,912000 & 370\,609118\,857298\,880000 \\ 3423\,706650 & 372\,533520\,586500 & 40\,535372\,375017\,065000 \\ 4108\,447980 & 99\,342272\,156400 & 2\,402096\,140741\,752000 \\ 3423\,706650 & 15\,920235\,922500 & 74029\,097039\,625000 \\ 1956\,403800 & 1\,455564\,427200 & 1082\,939933\,836800 \\ 733\,651425 & 68229\,582525 & 6\,345351\,174825 \\ \gamma_{9,1}(\mathfrak{x}_i) & \gamma_{9,2}(\mathfrak{x}_i) & \gamma_{9,3}(\mathfrak{x}_i) \\ 16\,303365 & 16\,303365 & 16\,303365 \end{pmatrix}$$

with integers

$$\begin{aligned} \gamma_{9,u}(\mathfrak{x}_i) &= \mathcal{P}_{0,9}(A)^{\cap}\cdot \odot^u\mathfrak{z}_9(\mathfrak{x}_i) \\ &= \mathcal{P}_{0,9}(A)^{\cap}\cdot \odot^u\bigl(\mathcal{P}_{9,10}(A)^{\cap}\cdot \mathfrak{x}_i^{\top}\bigr) \qquad \text{for} \quad 1 \le u \le 3. \end{aligned}$$

Only the numbers $\gamma_{9,u}(\mathfrak{x}_i)$ depend on the specific design, everything else is determined by the parameters of the design. The vectors $\mathcal{P}_{9,10}(A)^{\cap}\cdot \mathfrak{x}_i^{\top}$ for $i = 1, 2, 3$ are:

$\mathfrak{z}_9(\mathfrak{x}_1) = (2, 2, 9, 9, 11, 6, 9, 9, 7, 4, 8, 9, 7, 11, 10, 18, 9, 5, 7, 7, 9, 7,$
$12, 8, 8, 10, 8, 8, 8, 4, 5, 6, 8, 9, 8, 8, 8, 8, 10, 10, 8, 8, 9, 10, 10, 12,$
$8, 9, 9, 8, 12, 9, 9, 8, 8, 7, 8, 9, 9, 9, 7, 10, 7, 8, 11, 9, 6, 4, 6, 9, 3, 7,$
$7, 5, 9, 6, 10, 9, 9, 8, 7, 8, 9, 7, 7, 5, 7, 10, 6, 12, 10, 9),$
$\mathfrak{z}_9(\mathfrak{x}_2) = (2, 2, 9, 9, 11, 6, 8, 11, 7, 4, 8, 9, 7, 7, 14, 18, 9, 5, 8, 7, 7, 8,$
$9, 9, 8, 8, 7, 8, 8, 7, 7, 9, 9, 7, 10, 7, 9, 8, 7, 6, 8, 9, 9, 10, 6, 12, 8, 10,$
$11, 8, 12, 8, 8, 6, 7, 7, 10, 9, 7, 10, 7, 9, 9, 5, 6, 8, 7, 6, 6, 7, 7, 9, 9,$
$13, 7, 18, 7, 11, 0, 8, 11, 6, 13, 9, 7, 8, 7, 8, 9, 1, 10, 9),$
$\mathfrak{z}_9(\mathfrak{x}_3) = (2, 2, 9, 9, 11, 6, 7, 8, 8, 7, 8, 9, 6, 15, 10, 18, 8, 9, 9, 6, 8, 8,$
$12, 6, 8, 10, 7, 7, 8, 8, 7, 7, 8, 7, 8, 8, 8, 7, 10, 6, 7, 9, 8, 10, 8, 12, 7,$
$10, 10, 6, 9, 10, 6, 10, 8, 9, 8, 6, 11, 8, 11, 6, 7, 9, 9, 11, 10, 7, 7, 8, 5,$
$7, 9, 7, 7, 6, 7, 8, 9, 9, 5, 9, 10, 7, 13, 9, 7, 4, 6, 10, 6, 9).$

Thus we get

$\mathcal{D}_{\mathfrak{x}_1}$:	u	$\gamma_{9,u}(\mathfrak{x}_1)$	$\alpha_9^{(u)}(\mathcal{D}_{\mathfrak{x}_1})$
	1	163 033650	0
	2	1369 201800	603 084075
	3	11863 610100	1347 012000

$\mathcal{D}_{\mathfrak{x}_2}$:	u	$\gamma_{9,u}(\mathfrak{x}_2)$	$\alpha_9^{(u)}(\mathcal{D}_{\mathfrak{x}_2})$
	1	163 033650	0
	2	1377 385800	607 176075
	3	12092 018100	1380 988000

$\mathcal{D}_{\mathfrak{x}_3}$:	u	$\gamma_{9,u}(\mathfrak{x}_3)$	$\alpha_9^{(u)}(\mathcal{D}_{\mathfrak{x}_3})$
	1	163 033650	0
	2	1367 341800	602 154075
	3	11903 600100	1354 607000

As the values of $\alpha_9^{(2)}(\mathcal{D}_{\mathfrak{x}_i})$ are always different, we deduce that $\mathcal{D}_{\mathfrak{x}_1}$, $\mathcal{D}_{\mathfrak{x}_2}$ and $\mathcal{D}_{\mathfrak{x}_3}$ are pairwise nonisomorphic. Next, we display a table of all $\alpha_9^{(2)}(\mathcal{D}_{\mathfrak{x}_i})$ for $1 \leq$

$i \leq 138$. The tables displays the sorted values of $a_9^{(2)}(\mathcal{D}_{\mathfrak{X}_i})$. The indices i of the designs $\mathcal{D}_{\mathfrak{X}_i}$ are indicated afterwards.

591 366075 for {25}
593 226075 for {110}
594 342075 for {95}
595 830075 for {111}
596 853075 for {87}
597 039075 for {102}
597 225075 for {107}
597 318075 for {23, 128}
597 504075 for {5, 35}
597 597075 for {15, 46}
597 969075 for {8}
598 248075 for {126}
598 341075 for {14}
598 434075 for {118, 132}
598 527075 for {96}
598 806075 for {79}
598 899075 for {32, 70, 112}
598 992075 for {97, 100}
599 085075 for {48}
599 643075 for {49}
599 829075 for {44, 119}
599 922075 for {64}
600 015075 for {41}
600 108075 for {43}
600 201075 for {16, 122}
600 480075 for {75}
600 573075 for {89}
600 666075 for {134}
600 759075 for {7, 36, 68}
600 852075 for {106, 131}
601 131075 for {101, 103, 105}
601 224075 for {10}
601 317075 for {40}
601 503075 for {127}
601 689075 for {39, 120, 137}
601 782075 for {69}
601 968075 for {62, 88}
602 154075 for {3, 18, 45, 94}
602 433075 for {13, 109}
602 526075 for {66}
602 619075 for {93, 133}
602 712075 for {34}
602 805075 for {56, 57, 67}
602 898075 for {50, 61, 90}
602 991075 for {51, 86}
603 084075 for {1, 21, 54, 77, 108, 113}
603 177075 for {72}
603 270075 for {12, 59, 124}
603 363075 for {81, 117}
603 456075 for {84}
603 549075 for {65}
603 642075 for {91, 115, 116}
603 735075 for {104}
604 014075 for {22}
604 107075 for {26}
604 386075 for {11, 76, 129}

604 479075 for {31, 55}
604 665075 for {9, 136}
604 758075 for {29, 37}
604 944075 for {98}
605 223075 for {47}
605 316075 for {30}
605 409075 for {28}
605 595075 for {33, 73, 123}
605 967075 for {80}
606 153075 for {19, 92}
606 339075 for {53, 82, 85, 135}
606 525075 for {125}
606 618075 for {17, 121}
606 897075 for {60}
607 176075 for {2, 130}
607 641075 for {4, 6}
608 199075 for {114}
608 292075 for {38, 74}
608 385075 for {99}
608 478075 for {52}
608 571075 for {83}
608 664075 for {24, 42}
609 315075 for {20}
609 873075 for {27}
610 152075 for {78}
610 803075 for {58}
611 175075 for {63}
611 268075 for {71, 138}

We get the following sizes of classes: $1^{48}, 2^{23}, 3^{10}, 4^{2}, 6^{1}$. Another classification is obtained by considering $s = 3$. This classification is discrete, i. e. no two designs have the same intersection matrix $\mathcal{A}^{(3)}$. Thus, all 138 designs are nonisomorphic. As an example of how the classes of the $s = 2$ classification split, consider the largest class of size 6:

$$\{\mathcal{D}_{\mathfrak{F}_1}, \mathcal{D}_{\mathfrak{F}_{21}}, \mathcal{D}_{\mathfrak{F}_{54}}, \mathcal{D}_{\mathfrak{F}_{77}}, \mathcal{D}_{\mathfrak{F}_{108}}, \mathcal{D}_{\mathfrak{F}_{113}}\}.$$

All designs have $\alpha_9^{(2)}(\mathcal{D}_{\mathfrak{F}_i}) = 603\,084075$. The tuples $(\alpha_9^{(2)}(\mathcal{D}_{\mathfrak{F}_i}), \alpha_9^{(3)}(\mathcal{D}_{\mathfrak{F}_i}))$ for these designs are:

$$\begin{array}{llll}
(\,603\,084075\,, & 1341\,757500\,) & \text{for} & \mathcal{D}_{\mathfrak{F}_{108}}, \\
(\,603\,084075\,, & 1347\,012000\,) & \text{for} & \mathcal{D}_{\mathfrak{F}_{1}}, \\
(\,603\,084075\,, & 1350\,236000\,) & \text{for} & \mathcal{D}_{\mathfrak{F}_{21}}, \\
(\,603\,084075\,, & 1353\,382500\,) & \text{for} & \mathcal{D}_{\mathfrak{F}_{113}}, \\
(\,603\,084075\,, & 1360\,993000\,) & \text{for} & \mathcal{D}_{\mathfrak{F}_{77}}, \\
(\,603\,084075\,, & 1362\,419000\,) & \text{for} & \mathcal{D}_{\mathfrak{F}_{54}}.
\end{array}$$

The 1658 designs with $\lambda = 100$ can also be classified by their intersection numbers for $s \leq 3$.

Bibliography

[1] Martin Aigner. *Combinatorial theory. Repr. of the 1979 ed.* Classics in Mathematics. Springer, Berlin, 1997.

[2] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory.* Cambridge University Press, Cambridge, 1986.

[3] Anton Betten, Evi Haberberger, Reinhard Laue, and Alfred Wassermann. *DISCRETA – A program system for the construction of t-designs.* Lehrstuhl II für Mathematik, Universität Bayreuth, 1999. http://www.mathe2.uni-bayreuth.de/~discreta.

[4] Anton Betten, Adalbert Kerber, Reinhard Laue, and Alfred Wassermann. Simple 8-Designs with Small Parameters. *Designs, Codes, Cryptography*, 15:5–27, 1998.

[5] Anton Betten, Reinhard Laue, and Alfred Wassermann. Simple 6 and 7-designs on 19 to 33 points. *Congressus Numerantium*, 123:149–160, 1997.

[6] Anton Betten, Reinhard Laue, and Alfred Wassermann. Simple 7-Designs With Small Parameters. *J. of Combinatorial Designs*, 7:79–94, 1999.

[7] Jörn Bolick. t-designs und schnittzahlen, 1990. Master's Thesis, Universität Hamburg.

[8] P. J. Cameron and J. H. van Lint. *Designs, graphs, codes and their links*, volume 22 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[9] Charles J. Colbourn and Jeffrey H. Dinitz, editors. *The CRC handbook of combinatorial designs*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[10] Peter Dembowski. *Finite geometries*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Reprint of the 1968 original.

[11] Heinz-Richard Halder and Werner Heise. *Einführung in die Kombinatorik. Mit einem Anhang über formale Potenzen.* Carl Hanser Verlag, München - Wien, 1977.

[12] Shokichi (ed.) Iyanaga and Yukiyosi (ed.) Kawada. *Encyclopedic dictionary of mathematics. In two volumes. Transl. rev. by Kenneth O. May.* MIT Press, Cambridge, Massachusetts; London, 1980.

[13] Adalbert Kerber. *Applied finite group actions*. Springer, Berlin, Heidelberg, New York, 1999.

[14] T. P. Kirkman. On a problem in combinatorics. *Cambridge and Dublin Math. J.*, 2:191–204, 1847.

[15] T. P. Kirkman. Note on an unanswered price question. *Cambridge and Dublin Math. J.*, 5:255–262, 1850.

[16] T. P. Kirkman. Query iv. lady's and gentleman's diary., 1850.

[17] Donald E. Knuth. *The art of computer programming. Vol. 2.* Addison-Wesley Publishing Co., Reading, Mass., second edition, 1981. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[18] Egmont Köhler. Allgemeine Schnittzahlen in t-designs. In *Proceedings of the Oberwolfach Meeting "Kombinatorik" (1986)*, volume 73, pages 133–142, 1988/89.

[19] Earl S. Kramer and Dale M. Mesner. t-designs on hypergraphs. *Discrete Math.*, 15(3):263–296, 1976.

[20] Reinhard Laue. Halvings on small point sets. *Journal of Combinatorial Designs*, 97:233–241, 1999.

[21] Udi Manber. *Introduction to algorithms. A creative approach.* Addison-Wesley Verlag, Bonn etc., 1989.

[22] N. S. Mendelsohn. Intersection numbers of t-designs. In *Studies in Pure Mathematics (Presented to Richard Rado)*, pages 145–150. Academic Press, London, 1971.

[23] Wilhelm Plesken. Counting with groups and rings. *J. Reine Angew. Math.*, 334:40–68, 1982.

[24] Dijen K. Ray-Chaudhuri and Richard M. Wilson. On t-designs. *Osaka J. Math.*, 12:737–744, 1975.

[25] Bernd Schmalz. t-Designs zu vorgegebener Automorphismengruppe. *Bayreuth. Math. Schr.*, 41:1–164, 1992. Dissertation, Universität Bayreuth, Bayreuth, 1992.

[26] Michel Sebille. Designs: extensions et groupes primitifs, 1998. Diplomarbeit, Université Libre de Bruxelles.

[27] J. H. van Lint and R. M. Wilson. *A course in Combinatorics.* Cambridge University Press, Cambridge, 1992.

[28] Tran van Trung, Qiu-rong Wu, and Dale M. Mesner. High order intersection numbers of t-designs. *J. Statist. Plann. Inference*, 56(2):257–268, 1996. Special issue on orthogonal arrays and affine designs, Part II.

[29] Alfred Wassermann. Finding simple t-designs with enumeration techniques. *J. of Combinatorial Designs*, 6(2):79–90, 1998.

[30] R. et al. Wilson. Atlas of finite group representations., 1999. http://for.mat.bham.ac.uk/atlas/.

[31] Ernst Witt. Über Steinersche Systeme. *Abh. Math. Semin. der Universität Hamburg*, 12:265–275, 1938.

Index

$[x]^n$, *see* raising factorial

$[x]_n$, *see* falling factorial

$|| \cdot ||$, *see* type of a partition

$\binom{n}{a_1, a_2, \ldots, a_r}$, *see* multinomial coefficient

$\odot$, *see* Hadamard-Produkt

$\vdash$, *see* partition

$| \cdot |$, *see* weight of a partition

3-(8, 4, 1) design, 53

2-(15, 3, 1) design, 3

5-(24, 8, 1) design, 56, 104

8-(31, 10, λ) designs, 57–63, 108–118

group ring, *see* semigroup ring

$\mathcal{A}^{(s)}$, *see* matrix of global intersection numbers

$\mathcal{A}^{[s]}$, *see* matrix of global intersection numbers

$\alpha(B_0)$, *see* block intersection type

$\alpha_i(B_0)$, *see* block intersection number

$\alpha_i(M)$, *see* intersection numbers

$\alpha_i^{(s)}(M)$, *see* intersection numbers of higher order

$\alpha_i^{(s)}(\mathcal{D})$, *see* global intersection number of a design

$\alpha_i^{[s]}(\mathcal{D})$, *see* global intersection number of a design

α_{ijk}°, 72

$\alpha_{u,v,w}^{(i,j,k)\vee}$, 85

$\alpha_{u,v,w}^{(i,j,k)\wedge}$, 85

$\alpha_{u,v}^{(i,j)\vee}$, 85

$\alpha_{u,v}^{(i,j)\wedge}$, 85

absorption, 71

admissible parameters, 7

anti flag, 1

antichain, 70

automorphism
- of designs, 2

automorphism group
- of a design, 2

$\mathcal{B}$, *see* design

$\mathscr{B}$, *see* matrix of binomial coefficients

binomial coefficients
- matrix of the ~, 29

block, 1
- ~ intersection number, 32

~ intersection type, 32
block size, 2
bound, 70

chain, 70
complementary design, 6, 10
complete design, 6
conjugate partition, 16
cycle type, 18

$\mathcal{D}^c$, *see* complementary design
decomposition, 11
$\mathrm{der}_p\,\mathcal{D}$, *see* derived design
derived design, 7
Design
  one-block ~, 6
design, 2
  3-(8, 4, 1) ~, 53
  2-(15, 3, 1) ~, 3
  5-(24, 8, 1) ~, 56, 104
  8-(31, 10, λ) ~s, 57–63, 108–118
  automorphism, 2
  automorphism group, 2
  block intersection number, 32
  block size, 2
  complementary ~, 6, 10
  complete ~, 6
  construction of ~s, 49–57
  derived ~, 7
  index, 2
  intersection numbers
    global, 42–47, 99
    of higher order, 34–42
    ordinary, 32–33
  intersection type, 32
  isomorphic ~s, 2
  parameters, 2, 5–10
  parameters $\lambda_{i,j}$, 9
  point regularity, 2
  replication number, 2
  residual ~, 7
  Steiner system, 2
  supplementary ~, 6
  trivial ~, 6
  with respect to smaller t, 6
  Witt ~, 55, 104
diagram
  Ferrers ~, 16
difference partition, 18
DISCRETA, 53
$\Delta\lambda$, 7
$\mathcal{D} = (\mathcal{V}, \mathcal{B})$, *see* design

empty design, 6

factorial
  falling ~, 7, 24
  raising ~, 24
falling factorial, 7, 24
Ferrers diagram, 16

flag, 1

global intersection number of a design, 43
group action on poset, 70

Hadamard produkt, 80

ι, 79
incidence matrix, 1
incidence relation, 1
incidence structure, 1–5
  anti flag, 1
  block, 1
  design, 2
  flag, 1
  incidence matrix, 1
  point, 1
inclusion / exclusion principle, 9
index, 2
infimum, 70
intersection numbers, 32, 99
  computation, 97–108
  global, 42–47
    matrix of global $\sim$, 97
  of higher order, 34–42
  ordinary, 32–33
intersection type, 32
isomorphism
  of designs, 2

κ, *see* weight map
k, *see* block size
Kirkman, 3
Köhler, 33
  generalized $\sim$-equations, 40
Kramer, Earl S., 49

$L^{(i)}(\mathcal{L})$, *see* layer of a lattice
λ, *see* index
$\lambda_{i,j}^{(x)}$, 34
λ_i, 5
$\lambda_{\max}$, 6
lattice, 70
  $\sim$ action, 71
  $\sim$ of subgroups, 84
  $\sim$ of subsets, 84, 91–95
  layer, 85
  one element, 72
  rank function, 83
  zero element, 72
lattice action, 71
lattice of subsets, 91–95
layer
  of a lattice, 85
Lemma
  Plesken, 72
lemma
  inclusion / exclusion, 9
length of a partition, 14
$\lambda_{i,j}$, 9

$\ell(p)$, *see* length of a partition

M_{24}, *see* Mathieu group
Mathieu group, 55
matrix of binomial coefficients, 29
matrix of global intersection numbers, 97
Mendelsohn, 32
    generalized ∼-equations, 39
Mesner, Dale M., 35, 38–40, 49
multinomial coefficient, 17
Multinomial Theorem, 23
multiset, 11
    standard form, 11

ν, *see* weight function
number partition, 12

$\mathcal{O}_{i,j}$, 85
$o_{i,j}$, 85
one-block design, 6

$\Pi(N)$, *see* Partition
$\Pi(n)$, *see* partition
$\mathcal{P}(A)^{\vee}$, *see* Plesken matrix
$\mathcal{P}(A)^{\wedge}$, *see* Plesken matrix
parameters
    admissible, 7
    of a design, 2
    of designs, 5–10
part
    of a decomposition, 11
partial ordering, 69
partition, 11–29
    conjugate ∼, 16
    cycle type, 18
    diagram, 16
    difference ∼, 18
    length, 14
    number ∼, 12
    set ∼, 12
    standard form, 12
    type, 15
    weight, 14
Plesken, 72, 80
Plesken matrix
    $\mathcal{P}(A)^{\vee}$, 73
    $\mathcal{P}(A)^{\wedge}$, 73
Plesken ring, 78–83
    of the Dodecahedron, 83
point regularity, 2
poset, 69
    group action on ∼, 70

r, *see* replication number
raising factorial, 24
rank function
    of a lattice, 83
red $\mathcal{D}$, *see* design with respect to smaller t
replication number, 2

res$_p$ $\mathcal{D}$, *see* residual design
residual design, 7
$r(n, k)$, *see* Stirling number of the first kind, signless

schoolgirl's problem, 3
semigroup action, 69
semigroup ring, 44
set partition, 12
signless Stirling number of the first kind, 25
$s_1(n, k)$, *see* Stirling numbers of the first kind
$s_2(n, r)$, *see* Stirling number of the second kind
standard form
  of a multiset, 11
standard form of a partition, 12
Steiner system, 2
Stirling number
  first kind
    signless, 25
  second kind, 19
Stirling numbers
  of the first kind, 26
supp $\mathcal{D}$, *see* supplementary design
supplementary design, 6
supremum, 70

t, *see* point regularity
Theorem
  Multinomial Theorem, 23
  of Köhler, 33
  of Mendelsohn, 32
  of Plesken, 80
  of Tran van Trung, Qiu-rong Wu, Dale M. Mesner, 35, 40
  Tran van Trung, Qiu-rong Wu, Dale M. Mesner, 39
topological numbering, 73
Tran van Trung, 35, 38–40
trivial design, 6

$\mathcal{V}$, *see* design
v, *see* design

weight function
  ν, 98
weight map
  on $\mathbb{Z}[\mathfrak{P}(\mathcal{V})]$, 44
weight of a partition, 14
weight space $\mathcal{W}_v$, 45
Witt design, 55, 104
Wu, Qiu-rong, 35, 38–40

$\mathbb{Z}_s(A, \mathfrak{x})$, 100