Counting Idempotent Relations

Bericht-Nr. 2008-15

Florian Kammüller

ISSN 1436-9915

Abstract

This article introduces and motivates idempotent relations. It summarizes characterizations of idempotents and their relationship to transitive relations and quasi-orders. Finally it presents a counting method for idempotent relations and lists the results for up to 6 points.

Contents

Chapter 1

Introduction

An idempotent relation is one that is persistent under sequential relational composition. Sequential composition $r; s$ of two relations $r \subseteq A \times B$ and $s \subseteq B \times C$ is defined as $\{(x, y) \mid \exists\ z.\ (x, z) \in r \wedge (z, y) \in r\}$. A relation $r \subseteq A \times A$ is idempotent iff $r; r = r$.

In this paper we arrive at reducing the problem of counting idempotents to counting unlabelled and labelled partial orders and quasi-orders. The presented method works for counting labelled idempotents. For the unlabelled case it does not work. However, it arrives at counting a subclass of unlabelled idempotents, those that have a partial order kernel.

We reuse in this paper the following Sloane sequences [9] and their numbers: A000798 (labelled quasi-orders $\mathcal{Q}$), A001930 (unlabelled quasi-orders q), A001035 (labelled partial orders $\mathcal{PO}$), and A000112 (unlabelled partial orders po). We also use Stirling numbers of the second kind, A008277 and A008278. In the following we present a counting method for a new sequence, that of labelled idempotent relations $\mathcal{I}$.

This paper begins in Section 2 with notations, some facts that are needed about the automorphism group on partial orders, and a summary of previous results about idempotents that have been leading on to the counting formula presented in this paper. Then in Section 3 we present the theory that enables counting idempotents. We give the counting results for up to 6 points – as far as we have been able to calculate by hand. The method we present is suitable for being implemented as a computer program thereby increasing the number of points. In an appendix we give details of the calculation for up to 5 points, for the calculation of up to 6 points see the author's web page [6].

Chapter 2

Background

In the theory of software specification in particular in refinement theory we consider operations on a system specification as relations rather than functions. If an element of the domain of a relation is related to more than one element in the range this is viewed as non-determinism and more pragmatically as a choice or conscious loseness in specification. In order to build a proper calculus for specification languages, algebra for relations is needed. In an algebraic characterization of operation composition, idempotence enables to reduce doubles, e.g. $op_1; op_1; op_2 = op_1; op_2$.

In the paper [7] we presented a first approach to investigate the theory of idempotents using the Isabelle/HOL theorem prover. In [5] we used the example of idempotents as a basic application of interactive theorem proving to develop simple algorithms rigorously. There we constructed a generate-and-test method for idempotents. As generate-and-test is not efficient this method enables to count idempotents only up to five elements in reasonable time. Already for six we have a run time of roughly ten weeks. Nevertheless, our generate-and-test algorithm is valuable as a counting method as the implementation of the efficient test predicate is proved sound inside Isabelle/HOL. Therefore, we can use it here to verify our results.

The three main steps of characterizing finite idempotent relations presented in [7] and [5] are as follows. We use the notation $r(x)$ to abbreviate the relational image of r at x, i.e., $\{y \mid (x,y) \in r\}$. The set $\mathrm{fix}\ r$ annotates $\{x \in \mathrm{dom}\ r \mid (x,x) \in r\}$.

$$\text{Let } r \text{ be reflexive and transitive. Then } r \text{ is idempotent.} \tag{2.1}$$

$$\text{idempotent } r \quad \equiv \quad \begin{pmatrix} \forall x.\ r(x) = \bigcup y \in \mathrm{fix}\ r \cap r(x).\ r(y) \\ \text{transitive } r \end{pmatrix} \tag{2.2}$$

$$\text{idempotent } r \quad \equiv \quad \begin{pmatrix} \forall\ n \in N.\ r(n) = \bigcup x \in F \cap r(n).\ r(x) \\ r_F \text{ transitive} \\ \forall\ f \in F.\ \forall\ y \in N \cap r(f).\ r(y) \subseteq r(f) \end{pmatrix} \tag{2.3}$$

where $r_F = \{(x, y).\ (x, y) \in r \wedge x \in F\}$, $F = \text{fixp } r$, and $N = \text{dom } r \setminus F$ in (2.3). These three properties are mechanically verified in Isabelle/HOL [5]; the proof scripts are available at the author's web page [6].

A relation is called a quasi-order iff it is reflexive and transitive [8]. From (2.1) it follows immediately that a quasi-order is idempotent.

We annotate labelled quasi-orders with $\mathcal{Q}(n)$, unlabelled with $q(n)$, where n is the number of elements in the domain of the relation. To annotate the domain we sometimes use $\mathbb{N}_n$ because the initial segment of the naturals may well represent any set of (labelled) points. For conjunctions $p \wedge q$ we sometimes use two-dimensional depiction, i.e. $\binom{p}{q}$. For disjointness of two sets A, B, i.e., $A \cap B = \varnothing$, we write $A \diamond B$.

Counting partial orders

Partial orders have been subject to counting methods many times. Most recent advances are due to Pfeiffer and Brinkmann and McKay [1, 2, 3, 8]. In [8] counting different kinds of relations $\mathcal{R}$ — including transitive relations and quasi-orders — has been achieved using the automorphism group $\mathsf{Aut}(\mathcal{R})$. Using similar methods Brinkmann and McKay arrive at improving their earlier results [1] to up to 15 or 16 points [2].

In the following we introduce the relationship between unlabelled and labelled partial orders needed for counting idempotents. We deviate from the way Pfeiffer introduced automorphisms and partial orders using action groups as we need only some facts that can already be derived using equivalence relations and factorizations. For a deeper and more complete characterization of partial orders and automorphisms see Pfeiffer's paper [8].

Proposition 2.0.1. *The relation*

$$\sim \quad = \quad \{(x, y) \mid \exists\ \phi \in \mathsf{Aut}(\mathcal{PO}(n)).\ \phi(x) = y\}$$

is an equivalence relation on labelled partial orders $\mathcal{PO}(n)$. It partitions $\mathcal{PO}$ into its orbits with respect to the automorphism group. The factorization yields an isomorphism to the unlabelled partial orders.

$$\iota : \mathcal{PO}(n)/\sim \quad \cong \quad po(n) \tag{2.4}$$

Proof. The relation $\sim$ is *reflexive*, as for any $s \in \mathcal{PO}(n)$ we have id $s = s$ and id $\in \mathsf{Aut}(\mathcal{PO}(n))$. It is symmetric as with $f \in \mathsf{Aut}(\mathcal{PO}(n))$ also $f^{-1} \in \mathsf{Aut}\mathcal{PO}(n)$. Therefore, for any $s, s' \in \mathcal{PO}(n)$ iff $s \sim s'$, i.e., $f(s) = s'$ for some $f \in \mathsf{Aut}(\mathcal{PO}(n))$, then also $s' \sim s$, as $f^{-1}(s') = s$ and $f^{-1} \in \mathcal{PO}(n)$. Finally, we use the same proof with the argument $f_1, f_2 \in \mathsf{Aut}(\mathcal{PO}(n))$ implies $f_2 \circ f_1 \in \mathsf{Aut}(\mathcal{PO}(n))$ to prove transitivity of $\sim$. Hence $\sim$ constitutes an equivalence relation.

For the second part it follows immediately from the homomorphism theorems of universal algebra that the factorization $\mathcal{PO}(n)/\sim$ with the induced relation

$[x]_\sim \sim_\iota [y]_\sim$ iff $x \sim y$ is well-defined. The factorized relation is isomorphic to the unlabelled partial orders over n points $po(n)$ as any relation with the same graph but different order of nodes is contained in the same equivalence class. $\square$

We will usually write ζ for the natural epimorphism from $\mathcal{PO} \to \mathcal{PO}/\sim$ and $[s]_R$ to annotate a representant of the class of $s \in \mathcal{PO}$. The proposition immediately implies that – as $\sim$ constitutes a partitioning – we can count $\mathcal{PO}$ using the size of the orbits and the representatives from $\mathcal{PO}$. Let ι be the resulting isomorphism from $\mathcal{PO}(n)/\sim$ to $po(n)$ introduced in the previous proposition. The labelled partial orders $\mathcal{PO}(n)$ are a disjoint union of the equivalence classes of $\mathcal{PO}(n)/\sim$. We can build this union using ι as follows.

$$\mathcal{PO}(n) \quad = \quad \dot{\bigcup_{s \in po(n)}} \{r \in \mathcal{PO}(n) \mid \iota[r]_\sim = s\} \tag{2.5}$$

Hence the number of relations in $\mathcal{PO}(n)$ can be calculated from the cardinality of $po(n)$ and the size of the classes.

$$\#\mathcal{PO}(n) \quad = \quad \sum_{s \in po(n)} \#\iota^{-1}(s) \tag{2.6}$$

The number of elements in an equivalence class corresponds to the size of the orbit created by the automorphism group. If the size of the class $[s]_\sim$ is one, i.e., any automorphisms maps s to itself, then the size of the orbit is 1. The maximal number of elements of an orbit is $n!$ as this is the number of permutations of n elements, and hence also the maximal number of automorphisms for n elements. In the case of such a class $[s]_\sim$ with $n!$ elements each automorphism maps to a different relation – the orbit does not repeat elements. The other cases are all factors of $n!$ and may be calculated as follows.

First we introduce the notion of indistinguishability of subrelations of a labelled partial order $s \in \mathcal{PO}$. Indistinguishable subrelations are subsets of a relation s that are invariant under automorphisms. A family χ of sets χ_j, $j \in J$ with $\chi_j \subseteq s$ and $\chi_j \diamond \chi_k$ for $j \neq k \in J$ is a set of *indistinguishable* subrelations iff

$$\exists \phi \in \mathsf{Aut}(\mathcal{PO}(n)).\ \left(\begin{array}{c} \forall j \in J.\ \exists!\ k \in J.\ k \neq j \wedge \phi(\chi_j) = \chi_k \\ \forall (x,y) \in s \setminus \bigcup_{j \in J} \chi_j.\ \phi(x,y) = (\phi(x), \phi(y)) = (x,y) \\ \phi(s) = s \end{array} \right).$$

We consider only maximal indistinguishable sets of subrelations χ, i.e. if some subset $u \subseteq s$ is indistinguishable to some χ_j then there is a k such that $u = \chi_k$. Intuitively, indistinguishable subsets are subgraphs of a relation that may be exchanged without changing the relation. Concerning the cardinality of the orbits, it diminishes proportional with the factorial of the size of the sets of indistinguishable subsets. If there are indistinguishable subsets that contain smaller indistinguishable subsets than the reduction is proportional to the product of the smaller subrelations. Hence, for the calculation of the orbits we consider sets of minimal subrelations. Let $s \in po(n)$ and χ_j be a family of minimal indistinguishable subsets in s. Then the following inequality holds.

$$\#\iota^{-1}s \quad = \quad \frac{n!}{\prod_{j\in J}(\#\chi_j)!} \tag{2.7}$$

Finally, we need as a provisional step the relationship between quasi-orders and partial orders also presented in Pfeiffer's paper [8].

For any quasi-order $\sqsubseteq \in \mathcal{Q}(n)$ the symmetric core $\equiv$ of $\sqsubseteq$ is defined by

$$x \equiv y \quad \text{iff} \quad \left(\begin{array}{c} x \sqsubseteq y \\ y \sqsubseteq x \end{array} \right) .$$

As pointed out by Pfeiffer [8] the induced relation $\sqsubseteq_i$ on the classes of $\mathbb{N}_n/\equiv$ is a partial order. To count quasi-orders one can thus count the number of partitions of a set with n elements into k nonempty subsets and multiply with the number of partial orders, i.e.,

$$\#\mathcal{Q}(n) = \sum_{i=1}^{k} \left\{ \begin{array}{c} n \\ i \end{array} \right\} \#\mathcal{PO}(k)\,,$$

where the number of partitions is a Stirling number of the second kind (see the Appendix for the first few numbers).

A Stirling distribution for a partial order $s \in \mathcal{PO}(n)$ we call according to this the natural epimorphism $\mathcal{S} : \mathcal{Q}(n) \to \mathcal{PO}(n)$.

Chapter 3

Counting Idempotents

Our counting method for idempotents provides an efficient method for calculating the numbers of labelled idempotent relations by calculating partitions of partial orders and labelled quasi-orders. It is based on the basic construction idea that is already visible in properties (2.1) and (2.2) being made more precise in (2.3). Any quasi-order is an idempotent relation (2.1). Property (2.2) shows that an idempotent relation r over a base set A can be constructed starting from a quasi-order over a subset of A — the fixpoints of r — by selecting a *range extension* and a *domain extension*, i.e., by choosing the non-fixpoints that are elements of the ranges of the fixpoints (range extensions) and the non-fixpoints that share the ranges of fixpoints (domain extensions).

If an element n shares the range of a fixpoint f, i.e., $r(f) \subseteq r(n)$ we say n *hangs-onto* f in r. The hangs-onto relation of an idempotent s is a quasi-order order, and vice versa any quasi-order may be seen as a hangs-onto relation for some idempotents s. This is the key to our counting method for idempotents. As already noted in Section 2, the quasi-orders can be partitioned to partial orders by factorizing with the symmetric core $\equiv$. We use this simplification as well to partition idempotents according to the partial order representing the hangs-onto relationship of the fixpoints rather than the quasi-orders, as the symmetric core does not have much effect on idempotents. Taking as given the number of unlabelled partial orders representing the abstracted and factorized hangs-onto relation of a set of idempotents, we define the *alphabet* of choices of range extension, domain extension and range/domain extension represented by it — the latter is a combination according to property (2.3). The alphabet represents for each non-fixpoint all possibilities how it may be related to the partial order kernel of a relation. This alphabet enables the unique construction of idempotents. Its cardinality for each partial order kernel thus gives rise to counting idempotents.

The construction process starts from the quasi-order and the induced partial order that build the kernel of an idempotent.

Definition 3.0.2. *The $\mathcal{Q}$-kernel of an idempotent $s \in \mathcal{I}(n)$ is* $s \cap (\mathrm{fix}\ s \times$

fix s). *Similarly, the $\mathcal{PO}$-kernel is $\zeta(s \cap (\text{fix } s \times \text{fix } s))$ where ζ is the natural epimorphism. For the unlabelled cases we assume the corresponding definitions.*

The natural epimorphism may be continued on idempotents.

Definition 3.0.3. *Let $s \in \mathcal{I}(n)$, $k \in \mathcal{Q}(m)$, and $k' \in \mathcal{PO}(m')$, such that k is the $\mathcal{Q}$-kernel of s, and, k' the $\mathcal{PO}$-kernel of s, i.e. $\zeta(k) = k'$. The continuation $\hat{\zeta}$ is the extension of ζ to $\mathcal{I}(n)$, i.e. $\hat{\zeta}(s) = s/\zeta$.*

The order on s/ζ is the induced order $\hat{s}$ given as

$$([x], [y]) \in \hat{s} \quad \text{iff} \quad (x, y) \in s$$

which is well-defined as non-fixpoints are not part of the symmetric core. Otherwise, $(n, n') \in s$ and $(n', n) \in s$ for non-fixpoints n, n' would imply $(n, n) \in s$ and $(n', n') \in s$ because of transitivity and hence n, n' would be fixpoints.

We observe that idempotents are respected by the transition from quasi-orders to partial orders.

Proposition 3.0.4. *Let $s \in \mathcal{I}(n)$, and $t \in \mathcal{Q}(m)$ the $\mathcal{Q}$-kernel and $t' \in \mathcal{PO}(m')$ the $\mathcal{PO}$-kernel of s. Then $\hat{\zeta}(s) \in \mathcal{I}(n')$ for $n' = n - (m - m')$.*

Proof. For the kernel this property is already given by the Stirling properties (see Section 2). For the remaining cases of non-fixpoint z related to the kernel we use the above noted fact that non-fixpoints are not part of the symmetric core. Hence the idempotents properties follow immediately because whenever $(z, x) \in s$ then also $(z, y) \in s$ for all $y \equiv x$ because of transitivity. Also for the other direction (x, z). Hence, in the factorization, for all x, y, z, (x, y) and (y, z) iff (x, z) . The size of the base set is $n' = n - (m - m')$ again because the non-fixpoints are not part of the symmetric core, hence their classes are singleton. □

Definition 3.0.5. *(domain/range extension) Given a base set $\mathbb{N}_n$, a set of fixpoints $F \subseteq \mathbb{N}_n$, and a quasi-order or a partial order s on F, let $n \in \mathbb{N}_n \setminus F$ be some arbitrary non-fixpoint. Then*

- *a range extension r is a subset of F such that the extended relation $s \cup (r \times n)$ is idempotent, and*
- *a domain extension d is a subset of F such that the extended relation $s \cup (n \times d)$ is idempotent.*

A down-set is defined for any partial order $\sqsubseteq$ as a set d closed with respect to smaller elements, i.e., if $x \in d$ and $y \sqsubseteq x$ then $y \in d$. We write $\downarrow_{\sqsubseteq} d$ or if the relation is clear fom context just $\downarrow d$. Up-sets $\uparrow u$ are defined dually [4].

Lemma 3.0.6. *Let $F \subseteq \mathbb{N}_n$ be a set of fixpoints and $\mapsto$ be a partial order on F. Any $d \subseteq F$ is a domain extension iff $\uparrow_{\mapsto} d$ and any $r \subseteq$ is range extension r iff $\uparrow_{\mapsto} r$.*

Proof. Let d be a domain extension, $x \in d$, and $x \mapsto y$. If for a non-fixpoint n we have that $n \mapsto x$ then also $n \mapsto y$ because of transitivity, whence $y \in d$. Similarly, let r be a domain extension, $x \in r$ and $y \mapsto x$. If $x \mapsto n$ then again because of transitivity, we have also $y \mapsto n$ whereby again $y \in r$. The other direction follows for domain extension from (2.3) first conjunct and for range extension from transitivity. $\square$

Lemma 3.0.7. *Let $F \subseteq \mathbb{N}_n$ be a set of fixpoints, s be a partial order on F, $r, d \subseteq F$, and $n \in \mathbb{N}_n \setminus F$. Then $\uparrow_s d$, $\downarrow r_s$, $r \diamond d$, and $\forall\ x \in r, y \in d.\ (x, y) \in s$ iff $s \cup n \times d \cup r \times n$ is idempotent.*

Proof. Assuming an idempotent of the form $s \cup n \times d \cup r \times n$ we have by property (2.3) third conjunct that $s(n) \subseteq s(f)$ for any $f \in r$, i.e., for any x if $(n, x) \in s$ then $(f, x) \in s$. Let $f' \in d$. As $(n, f') \in s$ by assumption, we have $(f, f') \in s$. Since $f \in r$ was arbitrary, we have $\forall\ f \in r, f' \in d, (f, f') \in s$. For disjointness, assume $r \not\diamond d$. Then for any $x \in r \cap d$ we have by construction $(n, x) \in s$ and $(x, n) \in s$ which contradicts transitivity if n is a non-fixpoint. For $\uparrow_s d$ and $\downarrow_s r$ the arguments from the proof of Lemma 3.0.6 apply. $\square$

Definition 3.0.8 (Alphabet)**.** *Let s be a partial order in $\mathcal{PO}(n)$, and B its base set* ran s = dom s*. The alphabet (of possible choices to extend to an idempotent) for s is the following set.*

$$\mathcal{A}(s) = \{(r, d) \in \mathbb{P}(B) \times \mathbb{P}(B) \mid \downarrow_s r \wedge \uparrow_s d \wedge r \diamond d \wedge \forall x \in r, y \in d.(x, y) \in s\}$$

The alphabet entails the following four cases for any $(r, d) \in \mathbb{P}(B) \times \mathbb{P}(B)$:

$$\begin{pmatrix} r = \varnothing \\ d = \varnothing \end{pmatrix} \vee \begin{pmatrix} r = \varnothing \\ \uparrow_s d \end{pmatrix} \vee \begin{pmatrix} d = \varnothing \\ \downarrow_s r \end{pmatrix} \vee \begin{pmatrix} (r, d) \neq (\varnothing, \varnothing) \\ \uparrow_s d \wedge \downarrow_s r \\ r \diamond d \\ \forall x \in r, y \in d. \\ (x, y) \in s \end{pmatrix}.$$

In order to efficiently count we observe that labelled partial orders that belong to the same orbit with respect to the automorphism group have isomorphic alphabets.

Proposition 3.0.9. *Let $s, s' \in \mathcal{PO}(n)$ such that $s \sim s'$. That is, there is $f \in \mathsf{Aut}(\mathcal{PO}(n))$ with $f(s) = s'$. Now, let $\hat{f}$ be the pointwise continuation of f on alphabets, i.e., $f(r, d) = (f(r), f(d))$. Then for any $(r, d) \in \mathcal{A}(s)$ we have that $f(r, d) \in \mathcal{A}(s') = \mathcal{A}(f(s))$, i.e., the alphabets are isomorphic.*

Proof. Since f is an automorphism we have that $f(B) = B$, hence $f(r, d) \in \mathbb{P}(B) \times \mathbb{P}(B) = \mathbb{P}(f(B)) \times \mathbb{P}(f(B))$. Now, we consider the four cases implicit in the definition of alphabet. We show for each case that $f(r, d) \in \mathcal{A}(f(s))$. First, if $f(r, d) = (f(r), f(d)) = (\varnothing, \varnothing)$ then it is in $\mathcal{A}(f(s))$ as $(f(\varnothing), f(\varnothing)) = (\varnothing, \varnothing)$. If $(f(r), f(d)) = (\varnothing, f(d))$ and $f(d) \neq \varnothing$, then $r = \varnothing$ and $d \neq \varnothing$. Hence, as $(r, d) \in \mathcal{A}(s)$, we have that $\uparrow d$. As f is a homomorphism, we also have

$\uparrow f(d)$. Similarly, for $f(d) = \varnothing$ and $r \neq \varnothing$, we have $d = \varnothing$, $\downarrow r$, $r \neq \varnothing$, and $f(r) \neq \varnothing$. Again, as f is homomorphism, we have $\downarrow f(r)$. Finally, for $(f(r), f(d)) \neq (\varnothing, \varnothing)$, then also $(r, d) \neq (\varnothing, \varnothing)$. Therefore, as $(r, d) \in \mathcal{A}(s)$, $\forall\, x \in r, y \in d.\ (x, y) \in s$. Let $x' \in f(r)$ and $y' \in f(d)$ be arbitrary. Then as f is onto there are $x \in r$ and $y \in d$ with $f(x) = x'$, $f(y) = y'$, and $(x, y) \in s$. As f is homomorph $(f(x), f(y))$ in $f(s) = s'$. □

Proposition 3.0.9 simplifies the way we can count alphabet sizes. It suffices to construct and count the alphabet just for each representative of a class of partial orders $\iota^{-1}(s)_R$ where $s \in po(n)$ and ι the isomorphism introduced in (2.4).

Corollary 3.0.10. *For any alphabet size j and points k we have the following equality.*

$$\#\{x \in \mathcal{PO}(k) \mid \mathcal{A}(s) = j\} = \sum_{\substack{s \in po(k) \\ \mathcal{A}(\iota^{-1}(s)_R) = j}} \#\iota^{-1}(s)$$

To calculate the size of the classes we can use properties (2.6) and (2.7). A further observation that facilitates the counting of alphabets is that the number of down-sets (or pure range extensions) is equal to the number of up-sets (see the example calculation in the Appendix). Also, symmetric structures have equally sized alphabets.

An idempotent can be represented by its partial order kernel, a Stirling distribution and alphabet choices for each non-fixpoint.

Theorem 1 (Representation)**.** *For any labelled idempotent i over $\mathbb{N}_n$ with given fixpoints F and non-fixpoints N there are a unique Stirling distribution $\mathcal{S} : \mathcal{Q}(m) \to \mathcal{PO}(m')$, $s \in \mathcal{PO}(m')$, and $\alpha \in N \to \mathcal{A}(s)$. Vice versa, any such representation $(\mathcal{S}, s, \alpha)$ corresponds to one idempotent relation for F and N.*

Proof. Let $s_q \in \mathcal{Q}(m)$ be the $\mathcal{Q}$-kernel of i and $s \in \mathcal{PO}(m')$ be the corresponding $\mathcal{PO}$-kernel $\zeta(s_q)$. We show that the non-fixpoints can be uniquely represented by α with respect to the continuation $\hat{\zeta}(i)$. Proposition 3.0.4 grants that we can abstract from the symmetric core, here represented by $\mathcal{S}$. Let $n \in N$. Either $n \notin \text{dom } i \cup \text{ran } i$ then $\alpha(n) = (\varnothing, \varnothing)$. If $n \in \text{ran } i$ only, let r be the set of all fixpoints for which n is a range extension. By Lemma 3.0.6 we have $\downarrow r$. Similarly, if n is only in the domains of elements in d we have $\uparrow d$. Finally, if both cases are represented by (r, d) we have $\forall\, x \in r, y \in d.\ (x, y) \in s$ because of the third conjunct in property (2.3). Each of these cases corresponds to an element of $\mathcal{A}(s)$. Vice versa, we can construct an idempotent from the representation as

$$\mathcal{S}^{-1}(s) \cup \bigcup_{n \in N} n \times \mathcal{S}^{-1}(\pi_2(\alpha(n))) \cup \mathcal{S}^{-1}(\pi_1(\alpha(n))) \times n$$

where π_i are the projections of a pair to its i-th component. Idempotence of the constructed relation is a consequence of Proposition 3.0.4 together with Lemmata 3.0.6 and 3.0.7. □

For $n = 0$ and $n = 1$ the number of idempotents is 1. For any larger number the following theorem enables to count the number of labelled idempotents.

Theorem 2 (Number of labelled idempotents)**.** *The number of idempotent relations $\mathcal{I}(n)$ can be calculated for $n > 1$ as*

$$\#\mathcal{I}(n) = 1 + (\sum_{i=1}^{n-1} \binom{n}{i} \sum_{j=3}^{2^{i+1}-1} p_{ij} j^{n-i}) + \#\mathcal{Q}(n)$$

where the p_{ij} are given by the characteristic sequence

$$p_{ij} = \sum_{k=1}^{i} \left\{ \begin{matrix} i \\ k \end{matrix} \right\} \#\{s \in \mathcal{PO}(k) \mid \#\mathcal{A}(s) = j\}\,.$$

Proof. The 1 stands for the empty relation which is idempotent. Otherwise we partition the idempotents according to their numbers of fixpoints. If there are n fixpoints, that is, the relation is reflexive, then according to property (2.1), the number of labelled idempotents is given by the number of labelled quasi-orders $\mathcal{Q}(n)$. For any number of fixpoints i, $0 < i < n$, there are $\binom{n}{i}$ disjoint cases. For any selection of i fixpoints, the representation given by Theorem 1 yields for each of the $n-i$ non-fixpoints j selections if there is an alphabet with j elements represented by some $\mathcal{Q}$-kernel. So we need to know the number of labelled $\mathcal{PO}$-kernels that have an alphabet with j elements. Therefore the characteristic sequence p_{ij} counts the number of labelled partial orders that have alphabets with j elements. For i fixpoints the maximal cardinality of an alphabet is $2^{i+1} - 1$ for i unrelated points. The minimum is 3 as the full relation (on any set of fixpoints F) gives the alphabet $\{\varnothing, (F, \varnothing), (\varnothing, F)\}$. For any j, for which exist some partial orders s with $\#\mathcal{A}(s) = j$, we have to consider the distribution of the i fixpoints in $1 < k < i$ nonempty subsets where k corresponds to the number of points of the structures s with $\#\mathcal{A}(s) = j$. The Stirling coefficient represents the number of choices for the symmetric cores. □

With Theorem 2 we can count labelled idempotents given the alphabets for the partial order kernels for specific sizes j. For the latter we can use Corollary 3.0.10 in addition to construct the alphabet just once for each class of partial orders. For examples of the alphabets and calculations of the results up to 5, see the Appendix. In Table 3.1 we provide an overview over the results up to 6 together with the values for quasi-orders and partial orders and the numbers of all relations over n elements $\mathcal{R}(n) = \wp(\mathbb{N}_n \times \mathbb{N}_n)$ with $\#\mathcal{R}(n) = 2^{2^n}$ for comparison.

In the remainder of this section, we will briefly show in how far this method for counting labelled idempotents can be used for counting unlabelled ones.

The alphabets constructed for the labelled partial orders give rise to construct alphabets $a(s)$ of unlabelled $s \in po$. From those we can in a similar way derive the number of unlabelled idempotents that have a partial order kernel, i.e. where the symmetric core contains only singleton elements.

#	0	1	2	3	4	5	6
$\mathcal{R}$	1	2	16	512	65536	33554432	68719476736
$\mathcal{PO}$	1	1	3	19	219	4231	130023
po	1	1	2	5	16	63	318
$\mathcal{Q}$	1	1	4	29	355	6942	209527
q	1	1	3	9	33	139	718
$\mathcal{I}$	1	1	11	123	2360	73023	3494057

Table 3.1: Numbers of the examined relations up to 6

Theorem 3 (Number of unlabelled idempotents with *po*-kernel)**.** *The number of idempotents $i_{po}(n)$ whose q-kernel is already a partial order is given for $n > 1$ by*

$$\#i_{po}(n) = 1 + (\sum_{i=1}^{n-1} \sum_{j=3}^{2^{i+1}-1} \#\{s \in po(j) \mid \#a(s) = j\} \binom{n-i+j-1}{j-1}) + \#q(n)\,.$$

Proof. The formula derives in a similar way as that in Theorem 2. The choices for the non-fixpoints, however, are calculated as multisets: for each non-fixpoint it matters which alphabet-element is chosen but the order does not matter. Hence, a selection of $(n-i)$ non-fixpoints consists of a multiset with $n-i$ elements out of j possible alphabet elements. For the choices of i fixpoints $0 < i < n$ the order does not matter, hence we just sum up without binomial coefficient. □

The Stirling selection can unfortunately not be applied to derive fom this number the general number of unlabelled idempotents. The reason is that the reverse introduction of symmetric cores into the unlabelled partial order kernel may turn indistinguishable fixpoints into distinguishable sets of fixpoints. We believe it is not possible to generally calculate the numbers of unlabelled idempotents from the numbers of i_{po} as the distinguishability it too dependent on the inividual structure of an $s \in i_{po}$.

Chapter 4

Outlook and Conclusions

We have presented a counting method for labelled idempotent relations. This counting method reduces the problem to counting labelled quasi-orders, unlabelled and labelled partial orders, and constructing the alphabets for partial orders representing the kernel of an idempotent. For unlabelled idempotents we presented a partial result.

We have applied the presented counting method for labelled idempotents up to six points. The results are shown in Table 3.1 and the derivation steps are contained in the Appendix. The results are additionally verified by the mechanically proved generate-and-test method [5].

The calculation of the number of idempotents over n points as described in this paper is an algorithm that takes some representation of unlabelled partial orders over $m < n$ points, the number of labelled quasi-orders over n points, and outputs the number of labelled idempotents. The algorithm constructs the alphabets for each representant of a labelled partial orders and calculates the size of the orbit. Finally, it just calculates the number of idempotents using the formula of Theorem 2. We have not yet attempted to implement this algorithm. Such an implementation will certainly increase the number of points for which we can calculate the number of labelled idempotents, we believe up to more than 10. However, as we directly reuse the number of $\mathcal{Q}$ we cannot get further than 16 – which is the current state of the art for labelled quasi-orders [2].

Bibliography

[1] G. Brinkmann and B. D. McKay. Posets on up to 16 points, *Order* **19** (2002), pp 147–179.

[2] G. Brinkmann and B. D. McKay. Counting unlabelled topologies and transitive relations, *Journal of Integer Sequences* **8** (2005), Article 05.21.

[3] Joseph C. Culberson and Gregory J. E. Rawlins. New results from an algorithm for counting posets. *Order* **7** (1991), pp 361–374.

[4] R. A. Davey and H. A. Priestley. *Introduction to Lattices and Order, Second Edition.* Cambridge University Press, 2002.

[5] F. Kammüller. *Interactive Theorem Proving in Software Engineering.* Habilitationsschrift, Technische Universität Berlin, 2006.

[6] F. Kammüller. Web page at http://www.cs.tu-berlin.de/ ∼flokam, 2006.

[7] F. Kammüller and J. W. Sanders. Idempotent relations in Isabelle/HOL. *International Colloquium of Theoretical Aspects of Computing, ICTAC'04*, LNCS 3407, Springer 2004.

[8] Götz Pfeiffer. Counting transitive relations. *Journal of Integer Sequences* **7**, No. 3, (2004) Article 04.3.2.

[9] N. J. A. Sloane *The on-line encyclopedia of integer sequences.* Published electronically at http://www.research.att.com/∼njas/sequences, 2006.

Appendix

In this appendix we illustrate our counting method for labelled idempotents by giving the details of the calculation. The numbers of idempotents for $n \in \{0,1\}$ are $\#\mathcal{I}(0) = \#\{\varnothing\} = 1$ and $\#\mathcal{I}(1) = \#\{\{(a,a)\}\} = 1$.

Labelled idempotents with two elements $\mathcal{I}(2)$

Following Theorem 2 we need as input $\#\mathcal{Q}(2)$, which is 4 according to Sloane sequence A000798, see also Table 3.1.

Now the formula of Theorem 2 instantiates for 2 to:

$$\#\mathcal{I}(2) = 1 + \sum_{i=1}^{1} \binom{2}{i} \sum_{j=3}^{2^{i+1}-1} p_{ij} j^{2-i} + \mathcal{Q}(2) = 1 + 2p_{13}3 + 4$$

where p_{13} is given by:

$$\sum_{k=1}^{1} \left\{ \begin{matrix} 1 \\ k \end{matrix} \right\} \#\{s \in \mathcal{PO}(k) \mid \#\mathcal{A}(s) = 3\}] = \#\{s \in \mathcal{PO}(1) \mid \#\mathcal{A}(s) = 3\} .$$

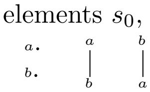
The set $\mathcal{PO}(1)$ is just the one point relation $o = \{(a,a)\}$. The alphabet over this relation is $\mathcal{A}(o) = \{(\varnothing,\varnothing),(\{a\},\varnothing),(\varnothing,\{a\})\}$. Since $\#\mathcal{A}(o) = 3$ we have that p_{13} is indeed 1, whereby

$$\#\mathcal{I}(2) = 1 + 6 + 4 = 11 .$$

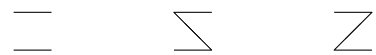
Labelled idempotents with three elements $\mathcal{I}(3)$

The unlabelled partial orders with two elements are the following. The labelled

versions are the following three elements s_0, s_1, and s_2.



We depict the order from top to bottom, for example, the middle one, say s_1, is the relation $\{(a,a),(a,b),(b,b)\}$. A more elaborate representation of the three relations s_0, s_1, and s_2 is given below where we can omit labels a and b as they are represented by positions top and bottom.



Although the second representation is graphically more elegant we use the first one for counting alphabets. The alphabet for the leftmost labelled partial order s_0 is:

$$\mathcal{A}(s_0) = \{(\varnothing,\varnothing),(\{a\},\varnothing),(\{b\},\varnothing),(\{a,b\},\varnothing),(\varnothing,\{a\}),(\varnothing,\{b\}),(\varnothing,\{a,b\})\}\,.$$

The number of elements of this alphabet is $\#\mathcal{A}(s_0) = 7$.

Next, we build the alphabet for s_1:

$$\mathcal{A}(s_1) = \{(\varnothing,\varnothing),(\{a\},\varnothing),(\{a,b\},\varnothing\},(\varnothing,\{b\}),(\varnothing,\{a,b\}),(\{a\},\{b\})\}\,.$$

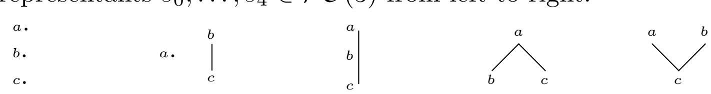
The orders s_1 and s_2 are both in the same equivalence class with respect to the natural isomorphism ζ (see Section 2). According to Proposition 3.0.9 it suffices to build one of the alphabets $\mathcal{A}(s_1)$ or $\mathcal{A}(s_2)$ as they are isomorphic and hence have the same number of elements. That is, $\#\mathcal{A}(s_1) = \#\mathcal{A}(s_2) = 6$.

The numbers p_{2j} for $3 \le j \le 7$ can now be calculated from these alphabet sizes. The characteristic number p_{23} is again 1 as $\#\{s \in \mathcal{PO}(1) \mid \#\mathcal{A}(s) = 3\}$ is one (see previous section) and $\left\{ {2 \atop 1} \right\}$ is also one. There is no element of $\mathcal{PO}(2)$ that has an alphabet with three elements. The sequence elements p_{24} and p_{25} are zero as there are again no structures in $\mathcal{PO}(1)$ or $\mathcal{PO}(2)$ with alpabets of those sizes. However, as we have have seen above there are structures s_1, and s_2 with alphabet size six. Hence p_{26} is two. For 7 the automorphism orbit contains only s_0, therefore p_{27} is 1. Summarizing, the number of idempotents with three elements can be calculated as follows.

$$\begin{aligned}
\#\mathcal{I}(3) &= 1 + \sum_{i=1}^{2} \binom{3}{i} \sum_{j=3}^{2^{i+1}-1} p_{ij} j^{3-i} + \#\mathcal{Q}(3) \\
&= 1 + \binom{3}{1} p_{13} 3^2 + \binom{3}{2} (3p_{23} + 6p_{26} + 7p_{27}) + 29 \\
&= 1 + 27 + 3(3 + 12 + 7) + 29 = 123
\end{aligned}$$

Labelled idempotents with four points $\mathcal{I}(4)$

The labelled partial orders with three elements are represented by the following five representants $s_0, \ldots, s_4 \in \mathcal{PO}(3)$ from left to right.



The alphabets and sizes of the orbits for each s_i are given in the following table. For brevity we write $\varnothing$ for $(\varnothing,\varnothing)$, S_r for $(S,\varnothing)$, S_d for $(\varnothing,S)$, and $\langle S_0,S_1\rangle_{rd}$ for (S_0,S_1) .

s_i	$\mathcal{A}(s_i)$	$\#\mathcal{A}(s_i)$	$\#\iota^{-1}(s_i)$
s_0	$\{\varnothing,\{a\}_d,\{b\}_d,\{c\}_d,\{a,b\}_d,\{a,c\}_d,\{b,c\}_d,\{a,b,c\}_d,$ $\{a\}_r,\{b\}_r,\{c\}_r,\{a,b\}_r,\{a,c\}_r,\{b,c\}_r,\{a,b,c\}_r\}$	15	1
s_1	$\{\varnothing,\{a\}_d,\{c\}_d,\{b,c\}_d,\{a,c\}_d,\{a,b,c\}_d,$ $\{a\}_r,\{b\}_r,\{a,b\}_r,\{b,c\}_r,\{a,b,c\}_r,\langle\{b\},\{c\}\rangle_{rd}\}$	12	6
s_2	$\{\varnothing,\{c\}_d,\{b,c\}_d,\{a,b,c\}_d,\{a\}_r,\{a,b\}_r,\{a,b,c\}_r,$ $\langle\{a\},\{c\}\rangle_{rd},\langle\{a\},\{b,c\}\rangle_{rd},\langle\{a,b\},\{c\}\rangle_{rd}\}$	10	6
s_3	$\{\varnothing,\{b\}_d,\{c\}_d,\{b,c\}_d,\{a,b,c\}_d,\{a\}_r,\{a,b\}_r,\{a,c\}_r,$ $\{a,b,c\}_r,\langle\{a\},\{b\}\rangle_{rd},\langle\{a\},\{c\}\rangle_{rd},\langle\{a\},\{b,c\}\rangle_{rd}\}$	12	3
s_4	$\{\varnothing,\{c\}_d,\{a,c\}_d,\{b,c\}_d,\{a,b,c\}_d,\{a\}_r,\{b\}_r,\{a,c\}_r,$ $\{a,b,c\}_r,\langle\{a\},\{c\}\rangle_{rd},\langle\{b\},\{c\}\rangle_{rd},\langle\{a,b\},\{c\}\rangle_{rd}\}$	12	3

As an illustration for sets of minimal indistinguishable subsets χ consider s_4: $\chi_1=\{\mathrm{a}\}$, $\chi_2=\{b\}$, hence $\iota^{-1}(s_4)=\frac{3!}{2!}=3$. Similarly for s_0 we have $\chi_1=\{a\}$, $\chi_2=\{b\}$, $\chi_3=\{c\}$ and $\iota^{-1}(s_4)=\frac{3!}{3!}=1$. From this table we can directly see that $p_{3,10}=6$, $p_{3,12}=12$, and $p_{3,15}=1$. The characteristic number p_{33} is again 1 as $\left\{{3 \atop 1}\right\}=1$. For p_{36} we get a nonzero in the sum only for 2, i.e.

$$\left\{{3 \atop 2}\right\}\#\{s\in\mathcal{PO}(2)\mid\#\mathcal{A}(s)=6\}=6\,.$$

For p_{37}, similarly,

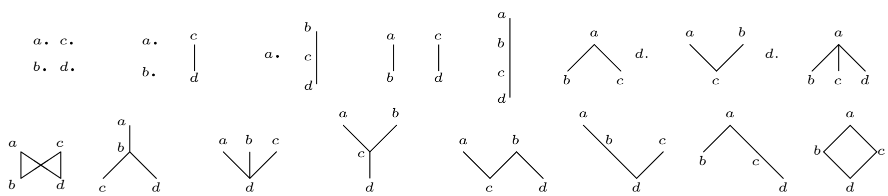
$$\left\{{3 \atop 2}\right\}\#\{s\in\mathcal{PO}(2)\mid\#\mathcal{A}(s)=7\}=3\,.$$

Now, the number of elements in $\mathcal{I}(4)$ can be calculated as follows.

$$\begin{aligned}
\#\mathcal{I}(4) &= 1+\sum_{i=1}^{3}\binom{4}{i}\sum_{j=3}^{2^{i+1}-1}p_{ij}j^{4-i}+\#\mathcal{Q}(4)\\
&= 1+\binom{4}{1}p_{13}3^3+\binom{4}{2}(3^2p_{23}+6^2p_{26}+7^2p_{27})+\\
&\quad\binom{4}{3}(3p_{33}+6p_{36}+7p_{27}+10p_{3,10}+12p_{3,12}+15p_{3,15})+355\\
&= 1+108+780+1116+355=2360
\end{aligned}$$

Labelled idempotents with five points $\mathcal{I}(5)$

The labelled partial orders with four elements are represented by the following 16 representants $s_0,\ldots,s_{15}\in\mathcal{PO}(4)$.



	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}
$\#\mathcal{A}(s_i)$	31	24	18	19	15	22	22	24	22	18	24	18	20	19	19	18
$\#\iota^{-1}(s_i)$	1	12	24	12	24	12	12	4	6	12	4	12	24	24	24	12

The new values for the characteristic sequence p_{4j}, $31 \geq j \geq 17$ are simply given by the sum of the orbits of all structures having j alphabet elements because $\left\{ {4 \atop 4} \right\} = 1$. Other new values are p_{4j} for $3 \leq j \leq 16$ given by additional multiplication with the corresponding Stirling numbers:

p_{43}	p_{46}	p_{47}	$p_{4,10}$	$p_{4,12}$	$p_{4,15}$
1	14	7	36	72	30

The case $p_{4,15}$ shows why we build the characteristic sequence by a sum over $k \in 1 \ldots i$. We can have partial orders with a different number of points and equal alphabet sizes: the relation $\{(a,a),(b,b),(c,c)\} \in \mathcal{PO}(3)$ and the above $s_4 \in \mathcal{PO}(4)$ have alphabet size 15, hence contribute to $p_{4,15}$.

$$\begin{aligned} p_{4,15} &= \left\{ {4 \atop 3} \right\} \#\{s \in \mathcal{PO}(3) \mid \#\mathcal{A}(s) = 15\} + \left\{ {4 \atop 4} \right\} \#\{s \in \mathcal{PO}(4) \mid \#\mathcal{A}(s) = 15\} \\ &= 6 + 24 = 30 \end{aligned}$$

The calculation of $\#\mathcal{I}(5)$ is now as follows.

$$\begin{aligned} \#\mathcal{I}(5) &= 1 + \sum_{i=1}^{4} \binom{5}{i} \sum_{j=3}^{2^{i+1}-1} p_{ij} j^{5-i} + \#\mathcal{Q}(5) \\ &= 1 + \\ &\quad \binom{5}{1} p_{13} 3^4 + \\ &\quad \binom{5}{2} (3^3 p_{23} + 6^3 p_{26} + 7^3 p_{27}) + \\ &\quad \binom{5}{3} (3^2 p_{33} + 6^2 p_{36} + 7^2 p_{37} + 10^2 p_{3,10} + 12^2 p_{3,12} + 15^2 p_{3,15}) + \\ &\quad \binom{5}{4} (3 p_{43} + 6 p_{46} + 7 p_{47} + 10 p_{4,10} + 12 p_{4,12} + 15 p_{4,15} + \\ &\qquad 18 p_{4,18} + 19 p_{4,19} + 20 p_{4,20} + 22 p_{4,22} + 24 p_{4,24} + 31 p_{4,31}) + \\ &\quad 6942 \\ &= 1 + 405 + 8020 + 29250 + 28405 + 6942 = 73023 \end{aligned}$$

Used Stirling numbers

The first few Stirling numbers $\left\{ {n \atop k} \right\}$ representing the partition of n elements into k parts are given in the following table.

$k \setminus n$	1	2	3	4	5
1	1	1	1	1	1
2		1	3	7	15
3			1	6	25
4				1	10
5					1