J Algebr Comb (2009) 30: 233–253
DOI 10.1007/s10801-008-0157-9

P-orderings of finite subsets of Dedekind domains

Keith Johnson

Received: 6 May 2008 / Accepted: 8 October 2008 / Published online: 3 November 2008

Abstract If R is a Dedekind domain, P a prime ideal of R and $S \subseteq R$ a finite subset then a P-ordering of S, as introduced by M. Bhargava in (J. Reine Angew. Math. 490:101–127, 1997), is an ordering $\{a_i\}_{i=1}^m$ of the elements of S with the property that, for each $1 < i \leq m$, the choice of a_i minimizes the P-adic valuation of $\prod_{j<i}(s - a_j)$ over elements $s \in S$. If S, S' are two finite subsets of R of the same cardinality then a bijection $\phi : S \to S'$ is a P-ordering equivalence if it preserves P-orderings. In this paper we give upper and lower bounds for the number of distinct P-orderings a finite set can have in terms of its cardinality and give an upper bound on the number of P-ordering equivalence classes of a given cardinality.

Keywords P-ordering · P-sequence · Dedekind domain

1 Introduction

Let R be a Dedekind domain, P a prime ideal of R, K the quotient field of R and q the cardinality of R/P. Also, for $x \in R$, let $\gamma(x)$ denote the largest integer k for which $x \in P^k$. If S is a subset of R then a P-ordering of S, as introduced in [1], is a sequence $\{a_i | i = 1, 2, \dots\}$ of elements of S with the property that, for each $i > 1$, the choice of a_i minimizes $\gamma(\prod_{j<i}(s - a_j))$ over all $s \in S$. Such orderings play a central role in the study of polynomials which are integer valued on subsets of R ([1], [2]). For S a finite set we will make the convention that a P-ordering of S stops when all elements of S have been enumerated (since beyond that point $\gamma(\prod(s - a_j)) = \infty$ for any $s \in S$ and the ordering is arbitrary). If S, S' are two finite subsets of R of the same cardinality, m, then a bijection $\phi : S \to S'$ is a P-ordering equivalence if $\{a_i\}_{i=1}^m$ is a P ordering of S if and only if $\{\phi(a_i)\}_{i=1}^m$is a P-ordering of S'.

K. Johnson (✉)
Department of Mathematics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada
e-mail: johnson@mathstat.dal.ca

Since the first element in a P-ordering can be picked arbitrarily it is clear that a set can have many different P-orderings and it is natural to ask how many distinct P-orderings a given finite set can have and how they can be enumerated. Similarly one can ask how many non P-ordering equivalent sets there are of a given cardinality, and how they can be enumerated. In this paper we give upper and lower bounds in terms of the cardinality of S for the number of P-orderings S can have and give an upper bound for the number non P-ordering equivalent sets that can exist of a given cardinality.

In more detail the results can be described as follows:

Proposition 1.1 *If $S \subseteq R$, is a set of cardinality m then S has at least 2^{m-1} P-orderings, and for each m there are sets realizing this bound.*

Proposition 1.2 *If $q = |P|$ then the maximum number of P-orderings which a subset of R of cardinality m can have is bounded by the function $\alpha(m)$ given by $\alpha(m) = m!$ for $m \leq q$ and for $m > q$*

$$\alpha(m) = max\{\prod_{i=1}^{q} i^{m_i} \prod_{i=1}^{q} \alpha(m_i)\}$$

where the maximum is taken over all sequences $m_1 \geq m_2 \geq \cdots \geq m_q \geq 0$ with $\sum m_i = m$ except the trivial sequence $m_1 = m$, $m_i = 0$ for $i > 1$.

The most familiar P-ordering is the usual increasing order on the set $\{1, \ldots, m\}$ in the case $R = \mathbb{Z}$. An analog of this set and ordering for a general Dedekind domain and prime P was defined in ([8], p.104). P-orderings of these sets have the following properties:

Proposition 1.3 *If $\{r_0, \ldots r_{q-1}\}$ is a set of representatives for R/P, π a representative of $P \setminus P^2$ and, for $n \in \mathbb{Z}^{\geq 0}$ whose representation in base q is $\sum n_i q^i$, $a_n = \sum r_{n_i} \pi^i$ then*

(a) The set $\{a_1 \ldots, a_m\}$ has $\beta(m)$ distinct P-orderings, where

$$\beta(m) = \prod_{n<m} (\prod_{i \geq 0} (n_i + 1))$$

(b) If $q = 2$ then $\alpha(m) = \beta(m)$, i.e. the sets in part (a) have the maximal number of P-orderings among sets of cardinality m.

(c) For each $q > 2$ there are sets of cardinality m with more than $\beta(m)$ P-orderings for infinitely many m.

Let $N(m)$ denote the number of P-ordering equivalence classes of sets of cardinality m.

Proposition 1.4 *The numbers $N(m)$ satisfy the inequality*

$$N(m) \leq \sum D(k_1 - 1, \ldots, k_t - 1) N(k_1) \ldots N(k_t)$$

where the sum is over all nontrivial partitions of m as a sum of no more than q strictly positive integers and $D(k_1, \ldots, k_t)$ denotes the generalized Delannoy number [7].

The proofs of these results are inductive and involve relating the P-orderings of S to those of certain of its subsets. This requires some algebraic and combinatorial results about combining orderings of subsets which we assemble in Section 2. The proofs of Propositions 1.1, 1.2 and 1.3 are then given in Sections 3. That section also contains remarks and computational results about the rate of growth of α and β. Section 4 contains the proof of Proposition 1.4.

The inequality in Proposition 1.4 is in most cases not an equality. In Section 4 we make some comments as to possible improvements and give some computational results for the case $R = \mathbb{Z}$ and $P = 2$ and 3.

It should be remarked that while the results in this paper hold for a general Dedekind domain the case of the integers illustrates almost all of the ideas completely. The only significant difference is that in the case of the integers q is a prime while in the general case it will be a power of a prime.

2 Shuffles and Alignments

We begin by establishing some elementary results about orderings, shuffles and alignments of finite collections of finite sets. In this paper it will be convenient for us to treat an ordered set as a finite sequence rather than as a set with a binary relation. We will use the notation $< n >$ to denote the set of integers from 1 to n (and take $< 0 >$ to be the empty set).

Definition 2.1 An ordering of a set S of cardinality n is a bijective map $\psi :< n > \to S$.

When only one ordering of a set is being considered we will sometimes revert to the familiar notation $\{a_i, i = 1, \ldots, n\}$ with $a_i = \phi(i)$ for an ordering. With this definition orderings pass to subsets as follows:

Definition 2.2 If S is an ordered set with ordering ψ, $S' \subseteq S$, and $i : S' \to S$ the inclusion map then the restriction of the ordering ψ to S' is the unique ordering ψ' of S' for which $\psi^{-1} \circ i \circ \psi'$ is increasing. ψ' is given by $\psi'(j) = s'$ if $j = |\{k \leq \psi^{-1}(s') | \psi(k) \in S'\}|$.

We will be concerned with the number of different ways in which a collection of ordered sets can be combined to form a larger ordered set. For this the following definition is useful.

Definition 2.3 Let $k_1, \ldots, k_q$ be nonnegative integers and $n = \sum k_j$. A $(k_1, \ldots, k_q)$-shuffle is an ordered set of q strictly increasing maps $\phi_j :< k_i > \to < n >$ with disjoint images.

In the special case $q = 2$ this is usually called a riffle shuffle and describes the familiar action of shuffling a deck of cards. There is a substantial literature on the algebra and combinatorics of this case [6]. In general a shuffle is sometimes also defined to be a permutation $\sigma \in S_n$ with the property that its restriction to each of the subsets $\{i \mid \sum_{\ell=1}^{j-1} k_\ell < i \leq \sum_{\ell=1}^{j} k_\ell\}$ is increasing. The correspondence between that definition and the one above is that if σ is such a permutation then $\phi_j(i) = \sigma(i + \sum_{\ell=1}^{j-1} k_\ell)$.

Proposition 2.4 (*a*) *If S is a finite ordered set with ordering ψ which is the disjoint union of subsets $S = \coprod_{j=1}^{q} S_j$ with $|S_j| = k_j$ and inclusion maps $i_j : S_j \to S$ then each S_j is, by restriction, an ordered set with ordering ψ_j and there exists a unique $(k_1, \ldots, k_q)$-shuffle $(\phi_1, \ldots, \phi_q)$ such that $\psi \circ \phi_j = i_j \circ \psi_j$ for $j = 1, \ldots, q$.*

(*b*) *If $\{(S_j, \psi_j), j = 1, \ldots, q\}$ is an ordered set of q finite ordered sets with $|S_j| = k_j$, $S = \coprod_{j=1}^{q} S_j$ and $(\phi_j, j = 1, \ldots, q)$ is a $(k_1, \ldots, k_q)$-shuffle then there is a unique order ψ for S such that $\psi \circ \phi_j = i_j \circ \psi_j$ for $j = 1, \ldots, q$.*

Proof (a) If $i_j : S_j \to S$ is the inclusion map then the map $\phi_j :< k_j > \to < n >$ is the strictly increasing map $\psi^{-1} \circ i_j \circ \psi_j$ in Definition 2.2. These maps have disjoint images because the S_j's are disjoint and the union of their images is $< n >$ because $\cup S_j = S$.

(b) The equation $\psi \circ \phi_j = i_j \circ \psi_j$ determines ψ uniquely because every integer in $< n >$ is in the image of ϕ_j for a unique index value j. The resulting map ψ is injective because each ψ_j and i_j is, and the i_j's have disjoint images. It is onto because ψ_j has image S_j and S is the union of the images of the i_j's. □

Terminology 2.5 If S, $\{S_j\}$, $\{\phi_j\}$ are related as in the previous lemma then we will refer to S as the ordered set obtained from $\{S_j\}$ by the action of the shuffle $\{\phi_j\}$, or as the shuffle of the $\{S_j\}$ if $\{\phi_j\}$ is clear from the context.

There is a similar definition and result for collections of sets which are not disjoint:

Definition 2.6 Let $k_1, \ldots, k_q$ be nonnegative integers and let $m \leq \sum k_j$. A $(k_1, \ldots, k_q; m)$-alignment is an ordered set of q strictly increasing maps $\phi_j :< k_i > \to < m >$ the union of whose images is $< m >$.

The name comes from applications in biology [9] of the case $q = 2$. The variation here is that the images of the ϕ_j's need not be disjoint. We will sometimes refer to such an object simply as a $(k_1, \ldots, k_q)$-alignment since the integer m can be recovered as the cardinality of the union of the images of the ϕ_j's.

Proposition 2.7 (*a*) *If S is a finite ordered set with ordering ψ and S is the union of subsets $S = \cup_{j=1}^{q} S_j$ with $|S_j| = k_j$, $|S| = m$ and inclusion maps $i_j : S_j \to S$ then each S_j is, by restriction, an ordered set with ordering ψ_j and there is a unique $(k_1, \ldots, k_q; m)$-alignment $(\phi_1, \ldots, \phi_q)$ such that $\psi \circ \phi_j = i_j \circ \psi_j$ for $j = 1, \ldots, q$.*

(*b*) *If $\{(S_j, \psi_j) | j = 1, \ldots, q\}$ is a collection of q finite ordered subsets of a set S with $|S_j| = k_j$, $S = \cup S_j$ and if $(\phi_1, \ldots, \phi_q)$ is a $(k_1, \ldots, k_q; m)$-alignment such that* *for any* $s \in S_j \cap S_{j'}$ $\phi_j \circ \psi_j^{-1}(s) = \phi_{j'} \circ \psi_{j'}^{-1}(s)$ *for any* j, j' *then there is a unique order* ψ *for* S *such that* $\psi \circ \phi_j = i_j \circ \psi_j$ *for* $j = 1, \ldots, q$.

Proof (a) As in the previous proof we take $\phi_j = \psi^{-1} \circ i_j \circ \psi_j$ which is strictly increasing. Since the ψ_j's are bijective and the union of the images of the i_j's is S, the union of the images of the ϕ_j's is $< m >$, hence these form an alignment.

(b) The equation $\psi \circ \phi_j = i_j \circ \psi_j$ determines ψ on the image of ϕ_j. An integer that is in the intersection of the images of two of the ϕ_j's is one whose inverse image under each of the ϕ_j's is mapped to the same element in S by each of the ψ_j's and so lies in the intersection of two or more of the S_j's. That this equation determines the same value for each of the possible choices of ϕ_j thus follows from the equation $\phi_j \circ \psi_j^{-1} = \phi_{j'} \circ \psi_{j'}^{-1}$ holding on the intersection of the S_j's. ψ is surjective because the ψ_j's are bijective and the union of the images of the i_j's is S. It is injective because each of the ψ_j's is. □

We will refer to the alignment determined in 2.7(a) as the union alignment of the S_r's.

A shuffle is, of course, a special case of an alignment but there is a further connection between the two ideas:

Proposition 2.8 *If* $\{\phi_1, \ldots, \phi_q\}$ *is a* $(k_1, \ldots, k_q)$*-shuffle with* $\sum k_j = n$ *and if* $\pi :< n > \to < m >$ *is a nondecreasing surjective map with the property that, for any* ℓ, $\pi^{-1}(\ell)$ *meets the image of any one of the* ϕ_j*'s in at most one point then* $\{\pi \circ \phi_1, \ldots, \pi \circ \phi_q\}$ *is a* $(k_1, \ldots, k_q; m)$*-alignment.*

Proof Since π is nondecreasing each $\pi \circ \phi_j$ is also nondecreasing. Since any $\pi^{-1}(\ell)$ meets the image of ϕ_j in at most one point, $\pi \circ \phi_j$ is injective and so strictly increasing. The union of the images of the $\bar{\phi}_j$'s is the image under π of the union of the images of the ϕ_j's, i.e. $\pi(< n >) =< m >$ since π is surjective. □

Definition 2.9 If π is as in the previous proposition then the alignment $\{\pi \circ \phi_1, \ldots, \pi \circ \phi_q\}$ will be called the projection of the shuffle $\{\phi_1, \ldots, \phi_q\}$ along π.

Proposition 2.10 *If* $\{\bar{\phi}_1, \ldots, \bar{\phi}_q\}$ *is a* $(k_1, \ldots, k_q; m)$*-alignment and* $\pi :< n > \to < m >$ *is a nondecreasing surjective map such that* $\sum k_j = n$ *and for every* $1 \le \ell \le m$ *it is the case that* $|\pi^{-1}(\ell)| = |\{j | \ell \in \text{Image}(\bar{\phi}_j)\}|$ *then the number of* $(k_1, \ldots, k_q)$*-shuffles whose projection along* π *is* $\{\bar{\phi}_1, \ldots, \bar{\phi}_q\}$ *is*

$$\prod_{\ell=1}^{m} |\pi^{-1}(\ell)|!$$

Proof Given $\{\bar{\phi}_1, \ldots, \bar{\phi}_q\}$ and π, choosing $\{\phi_1, \ldots, \phi_q\}$ such that $\bar{\phi}_j = \pi \circ \phi_j$ involves, for each $1 \le \ell \le m$, choosing values from $\pi^{-1}(\ell)$ for those ϕ_j's for which $\ell \in \text{Image}(\bar{\phi}_j)$. There are $|\pi^{-1}(\ell)|$ possible values and, by hypothesis, there are

$|\pi^{-1}(\ell)|$ such ϕ_j with $\ell \in \mathrm{Image}(\bar{\phi}_j)$, hence $|\pi^{-1}(\ell)|!$ ways of assigning the values to the ϕ_j's so that the images of the ϕ_j's are disjoint. That the resulting maps ϕ_j are increasing follows from the fact that the $\bar{\phi}_j$'s are and that π is nondecreasing. □

We note also that counting shuffles or alignments yields a familiar sequence of constants:

Proposition 2.11 (*a*) *The number of* $(k_1, \dots, k_q)$*-shuffles is the multinomial coefficient* $C(k_1, \dots, k_q) = (\sum k_j)!/(k_1! \dots k_q!)$.

(*b*) *The sum over m of the number of* $(k_1, \dots, k_q; m)$*-alignments for all* $m \le \sum k_j$ *is the generalized Delannoy number* [7] $D(k_1, \dots, k_q)$.

Proof (a) If $\{\phi_1, \dots, \phi_q\}$ is a $(k_1, \dots, k_q)$-shuffle with $\sum n_j = n$ then $n = \phi_j(k_j)$ for exactly one index value j and $\{\phi_1, \dots, \phi_j|_{<k_j-1>}, \dots, \phi_q\}$ is a $(k_1, \dots, k_j - 1, \dots, k_q)$-shuffle. Thus the number of $(k_1, \dots, k_q)$-shuffles, $C_{k_1,\dots,k_q}$ satisfies the recurrence

$$C(k_1, \dots, k_q) = \sum_{j=1}^{q} C(k_1, \dots, k_j - 1, \dots, k_q)$$

which is a familiar recurrence formula for the multinomial coefficients. As with the multinomial coefficients C also has the properties that $C(k_1, \dots, k_{i-1}, 0, k_{i+1}, \dots, k_q) = C(k_1, \dots, k_{i-1}, k_{i+1}, \dots, k_q)$ and that $C(k) = 1$. The result thus follows by induction.

(b) If $\{\phi_1, \dots, \phi_q\}$ is a $(k_1, \dots, k_q; m)$-alignment with $\sum n_j = m$ then $m = \phi_j(k_j)$ for some nonempty collection of index values. Let $\epsilon_j = 1$ if j is in this collection and 0 otherwise. It follows that $\{\phi_1|_{<k_1-\epsilon_1>}, \dots, \phi_q|_{<k_q-\epsilon_q>}\}$ is a $(k_1 - \epsilon_1, \dots, k_q - \epsilon_q)$-alignment and so that the number of $(k_1, \dots, k_q)$-alignments, $D(k_1, \dots, k_q)$, satisfies the recurrence

$$D(k_1, \dots, k_q) = \sum_{(\epsilon_1,\dots,\epsilon_q)\in(\{0,1\}^q)^*} D(k_1 - \epsilon_1, \dots, k_q - \epsilon_q)$$

where $(\{0, 1\}^q)^*$ denotes the set of all binary strings $(\epsilon_1, \dots, \epsilon_q)$ except $(0, \dots, 0)$. This is the recurrence determining the generalized Delannoy numbers. Both D and the Delannoy numbers have the properties $D(k_1, \dots, k_{i-1}, 0, k_{i+1}, \dots, k_q) = D(k_1, \dots, k_{i-1}, k_{i+1}, \dots, k_q)$ and $D(k) = 1$. Hence the result follows by induction. □

Remark The argument in the proof of part (b) of the previous proposition also gives the recurrence formula

$$D_(k_1, \dots, k_q; m) = \sum_{(\epsilon_1,\dots,\epsilon_q)\in(\{0,1\}^q)^*} D(k_1 - \epsilon_1, \dots, k_q - \epsilon_q; m - 1)$$

if $D(k_1, \dots, k_q; m)$ denotes the number of $(k_1, \dots, k_q; m)$ alignments. This allows the $D(k_1, \dots, k_q; m)$ to be computed recursively also. In particular for $q = 2$ it shows that

$$D(k_1, k_2; m) = \binom{k_2}{k_1 + k_2 - m}\binom{m}{k_2}$$

and so gives the well known formula ([5], p.81) for $D(k_1, k_2)$:

$$D(k_1, k_2) = \sum_m \binom{k_2}{k_1 + k_2 - m}\binom{m}{k_2}$$

3 Counting P-orderings

As in the introduction we define a P-ordering of a finite subset S of R as follows:

Definition 3.1 A P-ordering of S is an ordering $\{a_i, i = 1, 2, \dots |S|\}$ of S with the property that for each $i > 1$ the element a_i minimizes $\gamma(\prod_{j<i}(s - a_j))$ among all elements s of S.

Recall from [1] that there is associated to a set $S \subseteq R$ a sequence of nonnegative integers called the P-sequence of S.

Definition 3.2 If $\{a_i\}_{i=1}^m$ is a P-ordering of a set $S \subseteq R$ then the P-sequence of S is the sequence of integers $D = \{d_i\}_{i=1}^m$ with $d_1 = 0$ and $d_i = \gamma(\prod_{j<i}(a_i - a_j))$.

(In [2] the P-sequence of a set S is the sequence of ideals $(\prod_{j<i}(a_i - a_j))$ however in this paper there is one prime ideal P which is fixed throughout so that this is equivalent to working with the P-adic valuations of these ideals.) It is shown in [1] that the P-sequence of S depends only on S and not on the particular P-ordering used to compute it. We will find the following additional facts about P-sequences useful:

Lemma 3.3 (*a*) *The P-sequence of S characterizes P-orderings of S in the sense that if $\{a_i\}_{i=1}^m$ is an ordering of S such that $\gamma(\prod_{j<i}(a_i - a_j)) = d_i$ for all $1 \le i \le m$ then $\{a_i\}_{i=1}^m$ is a P-ordering of S.*

(*b*) *P-sequences are always nondecreasing.*

(*c*) *If $\pi \in P \setminus P^2$, $k \in \mathbf{Z}^+$, $r \in R$, $D = \{d_i\}_{i=1}^m$ is the P-sequence of S and $S' = \{r + \pi^k S \mid s \in S\}$ then the bijection $\phi(s) = r + \pi^k s$ between S and S' is a P-ordering equivalence of S and S' and the P-sequence of S' is $D' = \{d_i + i \cdot k\}_{i=1}^m$.*

Proof (a) Suppose that $\{a_i\}_{i=1}^m$ is an ordering of S for which $\gamma(\prod(a_i - a_j)) = d_i$ for all i. If $\{a_i\}_{i=1}^m$ were not a P-ordering, then there would exist $k > 1$ and $a \in R$ such that $\gamma(\prod_{j<i}(a_i - a_j))$ is minimal for $i < k$ and

$$\gamma(\prod_{j<k}(a - a_j)) < \gamma(\prod_{j<k}(a_k - a_j)) = d_k.$$

This contradicts the fact that d_k is the same for all P-orderings.

(b) The minimality of $\gamma(\prod_{j<k}(a_k - a_j))$ implies

$$d_k = \gamma(\prod_{j<k}(a_k - a_j)) \le \gamma(\prod_{j<k}(a_{k+1} - a_j)) \le \gamma(\prod_{j<k+1}(a_{k+1} - a_j)) = d_{k+1}$$

(c) Suppose $\{a_i\}_{i=1}^m$ is an ordering of S. The corresponding ordering of S' is $\{r + \pi^k a_i\}_{i=1}^m = \{a_i'\}_{i=1}^m$ and

$$\begin{aligned}\gamma(\prod_{j<i}(a_i' - a_j')) &= \gamma(\prod_{j<1}(\pi^k(a_i - a_j))\\ &= \gamma(\pi^{ik}\prod_{j<i}(a_i - a_j))\\ &= ik + \gamma(\prod_{j<i}(a_i - a_j)).\end{aligned}$$

Such an ordering is a P-ordering if and only if $\gamma(\prod_{j<i}(a_i' - a_j'))$ is minimal, which in turn happens if and only if $\gamma(\prod_{j<i}(a_i - a_j))$ is minimal since the term ik is constant for all i-fold products in S'. This formula also establishes the value of the P-sequence of S'. □

There is a connection between the P-sequence of a set S and that of certain of its subsets which will play a central role in what follows. The subsets of interest are:

Definition 3.4 If S is a finite subset of R and $r + P$ is a coset of R/P let $S_r = S \cap (r + P)$. If D is the P-sequence of S denote the P-sequence of S_r by D_r.

The following result relates P-orderings and the P-sequence of S to those of the S_r's. The first part of this result is Lemma 3.4 in [3] (see also [4]). We include a proof here for completeness.

Lemma 3.5 (*a*) *A P-ordering of S gives*, *by restriction*, *a P-ordering of S_r for each r*. *The P-sequence of S is equal to the sorted concatenation of the P-sequences D_r of the S_r's for all of the distinct residue classes of R/P where the sorting is into nondecreasing order.*

(*b*) *The P-sequence of each of the sets S_r is strictly increasing.*

Proof (a) Let $\{a_i\}_{i=1}^m$ be a P-ordering of S and suppose $a_k \in S_r$. If $a_j \in S_{r'}$ for $r \not\equiv r'(P)$ then $\gamma(a_k - a_j) = 0$, and so

$$\begin{aligned}d_k &= \gamma(\prod_{j<k}(a_k - a_j))\\ &= \gamma(\prod_{\substack{j<k\\ a_j \in S_r}}(a_k - a_j)).\end{aligned}$$

Furthermore if $s \in S_r$ then

$$\gamma\Big(\prod_{\substack{j<k\\ a_j\in S_r}} (s-a_j)\Big) = \gamma\Big(\prod_{j<k}(s-a_j)\Big) \geq \gamma\Big(\prod_{j<k}(a_k-a_j)\Big)$$

$$= \gamma\Big(\prod_{\substack{j<k\\ a_j\in S_r}} (a_k-a_j)\Big),$$

and so a_k minimizes $\gamma(\prod_{\substack{j<k\\ a_j\in S_r}} (s-a_j))$ for $s \in S_r$. Hence $\{a_i\}_{i=1}^m \cap S_r$ is a P-ordering of S_r and $\{d_k \mid a_k \in S_r\}$ is the P-sequence of S_r.

Since D is nondecreasing by Lemma 3.3(b), the result follows.

(b) In the proof of Lemma 3.3(b) the last inequality is strict for the sets S_r. □

In order to count the number of P-orderings a set can have we examine how we can reconstruct a P-ordering of S from that of the sets S_r in the previous lemma and for this the ideas of shuffle and alignment are relevant. Lemma 3.5(a) implies that a P-ordering of S is obtained from P-orderings of the sets S_r by applying a shuffle, and Lemma 3.3 identifies which shuffles of P-orderings of the S_r's yield P-orderings of S.

Lemma 3.6 *Suppose that $\{D_i, i = 1, \ldots, q\}$ is a set of finite sets of distinct nonnegative integers each with the increasing order, one for each $r \in R/P$. Let the cardinality of D_i be k_i and let D and $\bar{D}$ denote the disjoint union and the union respectively of the D_i's, each with the nondecreasing order. Also let the cardinalities of D and $\bar{D}$ be $n(=\sum k_i)$ and m respectively. In this case the inclusions $\bar{i}_i$ of the D_i's into $\bar{D}$ determine a $(k_1, \ldots, k_q)$-alignment and the canonical projection $\bar{\pi} : D \to \bar{D}$ determines a map $\pi :< n >\to< m >$. A $(k_1, \ldots, k_q)$-shuffle determines a shuffle of the D_i's into D if and only if it projects along π to the alignment determined by the D_i's.*

Proof The alignment is given by Proposition 2.7(a). Denote it by $(\bar{\phi}_1, \ldots, \bar{\phi}_q)$. It is determined by the condition that $\bar{i}_i \psi_i = \bar{\psi}\bar{\phi}_i$. Let ψ_i, ψ and $\bar{\psi}$ be the orders on D_i, D and $\bar{D}$. The map π is given by $\bar{\psi}^{-1}\bar{\pi}\psi$. A shuffle $(\phi_1, \ldots, \phi_q)$ projects along π to $(\bar{\phi}_1, \ldots, \bar{\phi}_q)$ if and only if $\pi\phi_i = \bar{\phi}_i$ for all i. It determines a shuffle of the D_i's into D if and only if $\psi\phi_i = i_i\psi_i$ for all i. Since $\bar{\pi}\psi = \bar{\psi}\pi$, $\bar{\pi}i_i = \bar{i}_i$ and ψ_i, ψ, $\bar{\psi}$

are bijections these are equivalent.

$$\begin{tikzcd}
D_i \arrow[dr, "i_i"] \arrow[dd, "\bar{i}_i"'] & & & k_i \arrow[lll, "\psi_i"'] \arrow[dl, "\phi_i"] \arrow[dd, "\bar{\phi}_i"] \\
& D \arrow[dl, "\bar{\pi}"] & < n > \arrow[l, "\psi"'] \arrow[dr, "\pi"] & \\
\bar{D} & & & < m > \arrow[lll, "\bar{\psi}"']
\end{tikzcd}$$

□

Proposition 3.7 *The following are equivalent*:

(*a*) *A shuffle of a collection of P-orderings of the S_r's results in a P-ordering of S.*

(*b*) *The shuffle of the associated D_r's results in a sequence in nondecreasing order.*

(*c*) *The shuffle projects along π to the alignment associated to the D_r's as in Lemma 3.6.*

Proof By Lemma 3.3 P-orderings of S are characterized by the P-sequence of S. Thus a shuffle yields a P-ordering of S if and only if the shuffle of the D_r's yields the P-sequence of S. This is described by Lemma 3.5. □

This Proposition gives us a method for inductively counting the number of P-orderings of a given set.

Corollary 3.8 *Let ℓ_i be the number of integers occurring in exactly i of the D_r's. There are $\prod_{i=1}^{q}(i!)^{\ell_i}$ distinct shuffles which shuffle the D_r's into the sequence D and so which shuffle P-orderings of the S_r's into a P-ordering of S.*

Proof From Lemma 3.5(a) the shuffles involved are those that shuffle the D_r's into a sequence in nondecreasing order. Since the D_r's are each strictly increasing the only choices in shuffling them into non decreasing order occur when the same integer occurs in more than one of the D_r's. If it occurs in i of them then there are $i!$ choices as to how to order them. □

Corollary 3.9 *If S_r has N_r distinct P-orderings for each residue class r, then S has*

$$\prod_{i=1}^{q}(i!)^{\ell_i}\prod_{r\in R/P}N_r$$

distinct P-orderings.

We may now prove Proposition 1.1 by induction:

Proof Suppose that for $n < m$ sets of cardinality n have at least 2^{n-1} P-orderings and that S is of cardinality m. By Lemma 3.3(c) S is P-ordering equivalent to a set containing representatives from at least two distinct residue classes modulo P and so, replacing S by this equivalent set if necessary, we may assume that S has this property. If S has representatives from k distinct residue classes modulo P then k of the P-sequences D_r of Lemma 3.7 have the number 0 in common and so in the previous corollary $\ell_k \geq 1$. Thus if $|S_j| = k_j$ so that $\sum k_j = m$ then the number of P-orderings of S is at least

$$k! \prod_{j=1}^{k} 2^{k_j - 1} = k! 2^{m-k} \geq 2^{m-1}.$$

To verify that this bound is sharp chose any strictly increasing sequence of nonnegative integers $\{e_j, j = 1, \ldots, m\}$ and consider the set $\{\pi^{e_j}\}$. This is P-equivalent to the set $\{\pi^{e_j - e_1}\}$ for which $|S_1| = 1$, $|S_0| = m - 1$ and $|S_r| = 0$ for all other residue classes r. Thus the number of P-orderings of S is twice that of S_0 by Corollary 3.9. Since S_0 is the same type of set as S with one fewer element, it follows by induction that S has 2^{m-1} P-orderings. □

Remark An entirely different proof of Proposition 1.1 can be given by showing that P-orderings of a finite set may be constructed in the reverse order by showing that a_j maximizes

$$\gamma(\prod_{s \in S \backslash \{a, a_{j+1}, \ldots, a_m\}} (a - s))$$

over all $a \in S \backslash \{a_{j+1}, \ldots, a_m\}$ and then showing that at every stage there are at least two elements that maximize this quantity.

Similarly we can establish Proposition 1.2:

Proof of Proposition 1.2 First note that if $m \leq q$ then any set of m elements in which no two are congruent modulo P will have all possible orderings as P-orderings. Thus we may assume $m > q$. Suppose that S^m is a set of cardinality m with the maximal number of P-orderings among sets of this size. If, as before, the intersections of S^m with the cosets of R/P are denoted S_r^m then the number of P-orderings of S^m is given by

$$\prod_{i=1}^{q} (i!)^{\ell_i} \prod_{r \in R/P} N_r,$$

where N_r, ℓ_i are as in Corollary 3.9. We may assume, by translating and removing common factors of P, that at least two of the sets S_r^m are nonempty. If we sort the sets S_r^m by size into decreasing order and let m_i denote the size of the i-th set then the product $\prod_{i=1}^{q} (i!)^{\ell_i}$ is largest for fixed m_i if each ℓ_i is as large as possible. Since

ℓ can be at most $m_i - m_{i+1}$, taking $m_{q+1} = 0$. In this case

$$\prod_{i=1}^{q}(i!)^{\ell_i} \leq \prod_{i=1}^{q}(\prod_{j=1}^{i} j)^{m_i - m_{i+1}} = \prod_{j=1}^{q}(j^{\sum_{i=j}^{q}(m_i - m_{i+1})}) = \prod_{j=1}^{q} j^{m_j}$$

and so the number of P-orderings is less than or equal to

$$\prod_{j=1}^{q} j^{m_j} \prod_{i=1}^{q} \alpha(m_i) \leq \alpha(m).$$

□

We next turn to the proof of Proposition 1.3

Proof of Proposition 1.3(a) If $m \leq q$ then all of the a_i are distinct modulo P and so all of the $m!$ possible orderings are P-orderings. Since for $m \leq q$ $\beta(m) = m!$ the result holds in these cases. Now assume $m > q$. As in the introduction let $a_n = \sum r_{n_i}\pi^i$ if the representation of n in base q is $\sum n_i q^i$ and let $S^m = \{a_1, \ldots, a_m\}$. Also, let $m = \ell \cdot q + t$ with $0 \leq t < q$. The sets S_r^m have $\ell + \delta$ elements for $\delta = 0$ or 1 with $\delta = 1$ if $r = r_k$ with $k < t$, and $\delta = 0$ otherwise. The bijection $S^{\ell+\delta} \to S_r^m$ given by $a \mapsto r + \pi a$ gives a $1-1$ correspondence between P-orderings of the two sets and also shows that the P-sequences of the S_r^m 's are all equal in the first ℓ entries, and those for which $\delta = 1$ have final entry equal also. Corollary 3.9 therefore implies that the number of P-orderings of S^m is equal to

$$(q!)^{\ell} \cdot t! \cdot (\#\text{ of } P\text{-orderings of } S^{\ell+1})^t \cdot (\#\text{ of } P\text{-orderings of } S^{\ell})^{q-t}.$$

Therefore to show that the number of P-orderings of S^m is $\beta(m)$ it suffices to show that $\beta(m)$ satisfies the recurrence

$$\beta(m) = (q!)^{\ell} t! \beta(\ell+1)^t \beta(\ell)^{q-t}.$$

Recall that

$$\beta(m) = \prod_{1 \leq n < m} (\prod_{i \geq 0}(n_i + 1)).$$

Lemma 3.10 *If* $0 < a < q$ *then*

$$\beta(aq^k) = (a!)^{q^k}(q!)^{kaq^{k-1}}.$$

Proof An integer i in the range from 0 to $a-1$ will occur as the $k+1$-st digit of the numbers in the range from 1 to $aq^k - 1$ exactly q^k times. Similarly for $0 \leq j \leq k$ an integer in the range from 1 to $q-1$ will occur as the j-th digit of numbers in the range from 0 to $aq^k - 1$ exactly aq^{k-1} times and 0 will occur $aq^{k-1} - 1$ times. Thus $\beta(aq^k) = (a!)^{q^k}((q!)^{aq^{k-1}})^k$. □

Corollary 3.11 $\beta(aq^k) = \beta(aq^{k-1})^q \cdot (q!)^{aq^{k-1}}$.

Lemma 3.12 *If* $0 < a < q$ *and* $aq^k < m \leq (a+1)q^k$ *then*

$$\beta(m) = (a+1)^{m-aq^k} \cdot \beta(aq^k) \cdot \beta(m-aq^k).$$

Proof For all n in the range $aq^k \leq n < m$ the $k+1$-st digit is a and the remaining digits coincide with those of $n - aq^k$. Thus

$$\begin{aligned}
\beta(m) &= \prod_{n<m}\Big(\prod_{i\geq 0}(n_i+1)\Big)\\
&= \prod_{n<aq^k}\Big(\prod_{i\geq 0}(n_i+1)\Big)\prod_{aq^k\leq n<m}\Big(\prod_{i\geq 0}(n_i+1)\Big)\\
&= \beta(aq^k)\prod_{aq^k\leq n<m}\Big(\prod_{i\geq 0}(n_i+1)\Big)\\
&= \beta(aq^k)(a+1)^{m-aq^k}\beta(m-aq^k).
\end{aligned}$$

□

We now verify the recurrence formula for β by induction on m and suppose $m = \ell q + t$ with $aq^k < m \leq (a+1)q^k$. Note that in this case $aq^{k-1} < \ell \leq (a+1)q^{k-1}$.

We then have, using the lemma twice and simplifying the result:

$$\begin{aligned}
&(q!)^\ell t!\beta(\ell+1)^t\beta(\ell)^{q-t}\\
&= (q!)^\ell t!(a^{\ell+1-aq^{k-1}}\beta(aq^{k-1})\beta(\ell+1-aq^{k-1}))^t\\
&\qquad \times(a^{\ell-aq^{k-1}}\beta(aq^{k-1})\beta(\ell-aq^{k-1}))^{q-t}\\
&= (q!)^\ell t!a^{t(\ell+1)+(q-t)\ell-qaq^{k-1}}\beta(aq^{k-1})^q\beta(\ell+1-aq^{k-1})^t\beta(\ell-aq^{k-1})^{q-t}\\
&= q!^\ell t!a^{m-aq^k}\beta(aq^{k-1})^q\beta(\ell+1-aq^{k-1})^t\beta(\ell-aq^{k-1})^{q-t}.
\end{aligned}$$

Using Corollary 3.11 this becomes

$$q!^{\ell-aq^{k-1}}t!a^{m-aq^k}\beta(aq^k)\beta(\ell+1-aq^{k-1})^t\beta(\ell-aq^{k-1})^{q-t}$$

which, by the induction hypothesis is

$$a^{m-aq^k}\beta(aq^k)\beta(m-aq^k) = \beta(m).$$

□

Proof of Proposition 1.3(b) If $m \leq q$ then $\alpha(m)$ and $\beta(m)$ are both equal to $m!$. To prove part (b) for $m > q$ it suffices to show that when $q = 2$ if $m = m_1 + m_2$ with $m_1 \geq m_2$ then $\beta(m) \geq 2^{m_2}\beta(m_1)\beta(m_2)$. Since for $q = 2$ the recurrence above for

$\beta(m)$ specializes to $\beta(2m)=2^m\beta(m)^2$ and $\beta(2m+1)=2^m\beta(m)\beta(m+1)$ we may prove this by induction on m. There are 4 cases according to the parities of m_1 and m_2. Suppose for example that m, m_1 and m_2 are all even, say $m_1=2m'$, $m_2=2m''$. Then

$$\begin{aligned}
2^{m_2}\beta(m_1)\beta(m_2) &= 2^{m_2+m'+m''}\beta(m')^2\beta(m'')^2\\
&= 2^{m'+m''}(2^{m''}\beta(m')\beta(m''))^2\\
&\le 2^{m'+m''}(\beta(m'+m''))^2\\
&= \beta(2(m'+m''))\\
&= \beta(m).
\end{aligned}$$

Similar calculations establish the other three cases. □

Proof of Proposition 1.3(c) To prove part (c) suppose $q>2$, let $\{r_i \mid i=1,\dots,q-1\}$ be any $q-1$ distinct residue classes in R/P and let $T=\{r_i,\pi+r_i \mid i=1,\dots,q-1\}$. Since this has 2 representatives from each of the residue classes r_i+P the number of distinct P-orderings of this set is $(q-1)!^2 2^{q-1}$. On the other hand $|T|=2(q-1)=q+(q-2)$ and $\beta(2(q-1))=q!(q-2)!2^{q-2}$ according to the recurrence for β. The ratio of these is $2-2/q>1$.

Define a sequence of sets T^n recursively by $T^0=T$, $T^{n+1}=\{\pi x+r \mid x\in T^n, r\in R/P\}$. The set T^n has $2q^n(q-1)$ elements and, using the recursive formula for the number of P-orderings,

$$(q!)^{(q^n(q-1)}((q-1)!)^{2q^n}2^{q^n(q-1)}$$

P-orderings. On the other hand

$$\begin{aligned}
\beta(q^n 2(q-1)) &= \beta(q^{n+1}+q^n(q-2))\\
&= 2^{q^n(q-2)}\beta(q^{n+1})\beta(q^n(q-2))\\
&= 2^{q^n(q-2)}(q!)^{(n+1)q^n}((q-2)!)^{q^n}(q!)^{n(q-2)q^{n-1}}.
\end{aligned}$$

The quotient of the number of P-orderings of T^n by $\beta(|T^n|)$ is $(2-2/q)^{q^n}$ which is greater than 1, and increases as n does. □

Lemmas 3.10 and 3.12 allow an explicit formula for $\beta(m)$ to be given in terms of the coefficients in the base q expansion of m and so give the upper bound $\beta(m)\le\, !^{m\log(m)/q\log(q)}$. For $q=2$ this gives a nonrecursive upper bound for α. For $q>2$ we have no such explicit formula for $\alpha(m)$. Some indication of the relation between $\alpha(m)$ and $\beta(m)$ for $q>2$ is given by the behaviour of $\log(\alpha(m)/\beta(m))$. Graphs of this function are given in Figure 1 for $q=3$ and $q=5$.

Proposition 3.7 gives a recursive method for enumerating the P-orderings of a given set S. If all elements of S lie in the same residue class modulo P then Lemma 3.3(c) can be applied to find a P-ordering equivalent set with representatives in at least two residue classes. The subsets S_r and their P-sequences, D_r, can

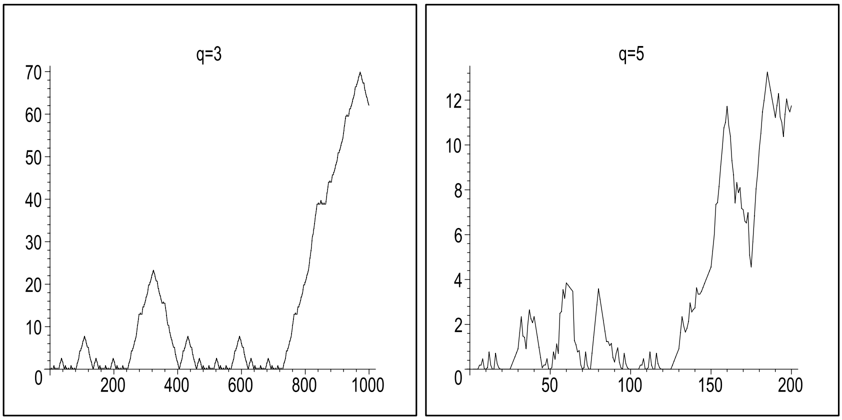

Fig. 1 $\log(\alpha(n)/\beta(n))$

be computed, the shuffles of the D_r's which result in a sequence in nondecreasing order can be enumerated, and the shuffles applied to the possible P-orderings of the S_r's. All of these calculations can be performed efficiently and the main impediment to applying this algorithm in practice is the amount of storage space required for the results.

4 Counting P-ordering equivalence classes

We would like now to consider counting the number of distinct P-ordering equivalence classes of a given size and to establish Proposition 1.4. That P-ordering equivalences can include more than affine maps is illustrated by the sets $\{0, 1, 2\}$ and $\{0, 1, 3\}$. Either of the maps taking 1 to 0 is a 2-order equivalence. On the other hand these sets are not 3-order equivalent since their intersections with the various residue classes modulo 3 are of different sizes. To analyze this situation we make use of Lemma 3.5 and for this it is necessary to know that P-ordering equivalences preserve the decompositions given by part (a) of that lemma.

Definition 4.1 A finite subset $S \in R$ will be called reduced if it is not contained in a single residue class modulo P.

Proposition 4.2 *If $S, S' \in R$ are finite reduced subsets and $\Phi : S \to S'$ is a P-ordering equivalence and if S_r, S'_r are the subsets of S, S' defined in Definition 3.4 then the restriction of Φ to any one of the S_r's is a P-ordering equivalence between S_r and $S'_{r'}$ for some residue class r'.*

Proof Let r be a residue class for which $S_r \neq \phi$. By hypothesis S_r^c, the complement of S_r is nonempty also. Choose $s \in S_r$. The set of elements $t \in S$ for which (s, t) begins a P-ordering of S is exactly S_r^c and so Φ, being a P-ordering equivalence, must map this set bijectively to the set of elements $t' \in S'$ for which $(\Phi(s), t')$ begins a P-ordering of S'. If $\Phi(s) \in S'_{r'}$ then this set is $(S'_{r'})^c$. Since Φ is a bijection this implies

$\Phi(S_r) = S'_{r'}$. Since every P-ordering of S_r occurs as the restriction of a P-ordering of S and similarly for $S'_{r'}$ and S' and Φ gives a bijection between P-orderings of S and of S', it must restrict to give a bijection between P-orderings of S_r and $S'_{r'}$. □

Corollary 4.3 *If S, S' are as above then a P-ordering equivalence determines a permutation σ of the residue classes modulo P such that $\Phi_r : S_r \to S'_{\sigma(r)}$ is a P-ordering equivalence for all r.*

It is clear from part (c) of Lemma 3.3 that P-ordering equivalent sets may have differing P-sequences. Non P-ordering equivalent sets may have equal P-sequences, however. For example the sets $\{0, 1, 2, 4\}$ and $\{0, 1, 3, 8\}$ in $\mathbb{Z}$ both have the 2-sequence $(0, 0, 1, 3)$ but can be seen to not be 2-order equivalent by comparing the size of the subsets S_r. What will serve as a means of classifying P-ordering equivalence classes is the P-equivalence classes of the subsets S_r together with the union alignment of the D_r's as described in Proposition 2.7(a).

Proposition 4.4 *Suppose that S and S' are reduced subsets of R and that for each residue class r there is a $\sigma(r)$ and a P-ordering equivalence $\Phi_r : S_r \to S'_{\sigma(r)}$ where σ is a permutation of the set of residue classes modulo P. Let D_r and $D'_{\sigma(r)}$ denote the P-sequences of S_r and $S'_{\sigma(r)}$. The bijections Φ_r together define a bijection $\Phi : S \to S'$ and Φ is a P-ordering equivalence if and only if the alignments determined by the ordered sets $\{D_r\}$ and $\{D'_{\sigma(r)}\}$ via Proposition 2.7(a) are equal.*

Proof Fix a P-ordering of each of the S_r's. By Proposition 3.7 a shuffle of these P-orderings gives a P-ordering of S if and only if this shuffle projects to the union alignment of the D_r's. If Φ is a P-ordering equivalence then this shuffle gives a P-ordering of S' and so projects to the union alignment of the $D'_{\sigma(r)}$.

Conversely suppose that the two P-alignments are equal. Then the collections of shuffles which project to each of them are equal also. Since a P-ordering of S is the shuffle of a collection of P-orderings of the S_r's by one of these shuffles and each Φ_r is a P-ordering equivalence, the image of this P-ordering under Φ must be a P-ordering of S'. □

We may now give a proof of Proposition 1.4.

Proof We begin with two observation about the coefficient $D(k_1 - 1, \dots, k_t - 1)$ occurring in the sum in the statement of Proposition 1.4. First, note that this coefficient is equal to the number of $(k_1 - 1, \dots, k_t - 1)$ alignments but that it also equals the number of $(k_1, \dots, k_t)$ alignments $(\phi_1, \dots, \phi_t)$ with the property that $\phi_i(1) = 1$ and $\phi(2) > 1$ for $i = 1, \dots, t$ since there is an obvious bijection between these sets. It is alignments of the second sort which occur in the proof below. Next, note that if we make the convention that $D(x_1, \dots, x_i, -1, x_{i+1}, \dots, x_t) = D(x_1, \dots, x_i, x_{i+1}, \dots, x_t)$ and that $N(0) = 1$ then we may take the sum in Proposition 1.4 to be over all decompositions of m of length q excepting the trivial decomposition $m = m + 0 + \cdots + 0$, i.e. take $t = q$. In this sum permutations of a decomposition are not enumerated separately hence this is the same as the sum over the set $\{(k_1,\dots,k_q)|\sum k_i = m, 0 \le k_1 \le k_2 \le \cdots \le k_q < m\}$.

To prove the proposition it suffices to exhibit an injective map, $\bar{\chi}$, from the set of P-ordering equivalence classes of size m to the set of pairs $(\Phi, \mathcal{S})$ consisting of a $(k_1,\dots,k_q)$-alignment, Φ, of the sort described above and a q-tuple of P-ordering equivalences classes of sizes $k_1,\dots,k_q$. Fix an ordering, $r_1,\dots,r_q$, for the elements of R/P. Given a P-ordering equivalence class of size m pick a reduced representative, S. Let $\mathcal{S}$ be the q-tuple of p-ordering equivalence classes of the sets S_r with the ordering for the elements of R/P fixed above. Let $k_i = |S_{r_i}|$. The P-sequences of the S_r's determine a union alignment, Φ. This is a $(k_1,\dots,k_q)$-alignment and since each of the P-sequences begins with 0 and is strictly increasing Φ is an alignment of the sort described above. Let $\chi(S) = (\Phi, \mathcal{S})$ and take $\bar{\chi}([S]) = \chi(S)$ where $[S]$ denotes the P-ordering equivalence class of S. Proposition 4.4 shows that sets for which the S_r's are P-ordering equivalent and the alignments are equal are themselves P-ordering equivalent. Thus $\bar{\chi}$ injective. Since the number of possible alignments is given by Proposition 2.11(b) the result follows. □

This result overestimates the number of P-ordering equivalence classes by counting some classes repeatedly. It is possible for two sets S and S' in the same P-ordering equivalence class to determine pairs $(\Phi, \mathcal{S})$, $(\Phi', \mathcal{S}')$ in which the alignments are not equal. The choice of a reduced representative in the definition of $\bar{\chi}$ determines which of these would lie in the image of $\bar{\chi}$. For example if $m = 4$ and $P = 2$ in $\mathbb{Z}$ then $S = \{0, 1, 3, 4\}$ and $S' = \{0, 1, 2, 5\}$ are 2-ordering equivalent (via the map $f(0) = 1$, $f(1) = 0$, $f(3) = 2$, $f(4) = 5$). The decompositions of S and S' with respect to the residue classes modulo P are $\mathcal{S} = (\mathcal{S}_0, \mathcal{S}_1) = ((0, 4), (1, 3))$ and $\mathcal{S}' = (\mathcal{S}'_0, \mathcal{S}'_1) = ((0, 2), (1, 5))$. Their P-sequences, $D = (0, 0, 1, 2)$ and $D' = (0, 0, 1, 2)$, decompose as $(D_0, D_1) = ((0, 2), (0, 1))$ and $(D'_0, D'_1) = ((0, 1), (0, 2))$ hence the alignments for these sets are $\Phi = ((1, 3), D'_1(1, 2))$ and $\Phi' = ((1, 2), (1, 3))$ and so only one of the pairs $(\Phi, \mathcal{S})$ or $(\Phi', \mathcal{S}')$ will occur in the image of $\bar{\chi}$. In general if $\sigma \in \Sigma_q$ is a permutation which preserves the decomposition $(k_1,\dots,k_q)$, i.e. $k_i = k_{\sigma(i)}$ for all i, and if S, S' are such that $\chi(S) = (\Phi, \mathcal{S}) = ((\phi_1,\dots,\phi_q), (\mathcal{S}_1,\dots,\mathcal{S}_q))$ and $\chi(S') = (\Phi', \mathcal{S}') = ((\phi_{\sigma(1)},\dots,\phi_{\sigma(q)}), (\mathcal{S}_{\sigma(1)},\dots,\mathcal{S}_{\sigma(q)}))$ then S and S' will be P-ordering equivalent while $(\Phi, \mathcal{S})$ and $(\Phi', \mathcal{S}')$ may be distinct and so only one of them in the image of $\bar{\chi}$. A more precise but less easily computable upper bound for $N(m)$ is obtained by taking into account this action of the symmetric group, Σ_q.

Proposition 4.5 *The number of P-ordering equivalence classes of sets of size m is less than or equal to the number of orbits of pairs $(\Phi, \mathcal{S})$ of a $(k_1,\dots,k_q)$-alignment Φ and q-tuples of P-orderings $\mathcal{S}$ of sizes $k_1,\dots,k_q$ with $\sum k_i = m$ under the action of elements of the symmetric group Σ_q preserving the decomposition $(k_1,\dots,k_q)$.*

Proof The map $\bar{\chi}$ in the previous proof has at most one element of each orbit in its image. □

For a given prime ideal P this observation can be used to add correction terms to the sum in Proposition 1.4. The formulas become increasingly complicated with the size of q as they require an enumeration of the possible orbit types, the number of which increases with q. We give below the cases $q=2$ and $q=3$.

Proposition 4.6 *The number of distinct* 2*-equivalence classes of subsets of* $\mathbb{Z}$ *of cardinality* m, $N(m)$ *satisfies the inequality*

$$\begin{aligned} N(m) \leq & \sum_{a+b=m, 0<a\leq b} D(a-1, b-1)N(a)N(b) \\ & - \delta_2(m)\frac{1}{2}(D(\frac{m}{2}-1, \frac{m}{2}-1)N(\frac{m}{2})^2 - N(\frac{m}{2})), \end{aligned}$$

where $\delta_2(m) = 1$ *if* m *is even and* 0 *if* m *is odd.*

Proof If m is even, $m = 2k$, then pairs of a (k,k)-alignment, (ϕ_0, ϕ_1), and a pair of 2-ordering equivalence classes, $(\mathcal{S}_0, \mathcal{S}_1)$, will lie in orbits of size 2 under the action of Σ_2 unless $\phi_0 = \phi_1$ and $\mathcal{S}_0 = \mathcal{S}_1$. There are $D(m/2-1, m/2-1)N(m/2)^2$ of the former and $N(m/2)$ of the later. □

This gives the following table of values which is sharp for $m \leq 6$:

m	1	2	3	4	5	6	7	8
$N(m)$	1	1	1	3	8	36	≤ 183	< 1192

Proposition 4.7 *The number of distinct* 3*-equivalence classes of subsets of* $\mathbb{Z}$ *of cardinality* m, $N(m)$ *satisfies the inequality*

$$\begin{aligned} N(m) \leq & \sum_{a+b+c=m, 0<a\leq b\leq c} D(a-1, b-1, c-1)N(a)N(b)N(c) \\ & + \sum_{a+b=m, 0<a\leq b} D(a-1, b-1)N(a)N(b) \\ & - \sum_{2a+b=m} \frac{1}{2}(D(a-1, a-1, b-1)N(a)^2 - D(a-1, b-1)N(a))N(b) \\ & - \delta_3(m)(\frac{5}{6}(D(\frac{m}{3}-1, \frac{m}{3}-1, \frac{m}{3}-1)N(m/3)^3 \\ & \quad - \frac{1}{2}D(\frac{m}{3}-1, \frac{m}{3}-1)N(\frac{m}{3})^2 - \frac{1}{3}N(\frac{m}{3})) \\ & - \delta_2(m)\frac{1}{2}(D(m/2-1, m/2-1)N(n/2)^2 - N(m/2)), \end{aligned}$$

where $\delta_3(m) = 1$ *if* m *is divisible by* 3 *and* 0 *otherwise and* $\delta_2(m)$ *is as in the previous proposition.*

Proof If m is divisible by 3 and $m = 3k$ then pairs of a (k,k,k)-alignment $\Phi = (\phi_0, \phi_1, \phi_2)$ and a triple of 3-ordering equivalence classes, $\mathcal{S} = (\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2)$, will lie

Table 1

S	D	S_0	D_0	S_1	D_1	(ϕ_0, ϕ_1)
{0}	(0)	{0}	(0)			
{0,1}	(0,0)	{0}	(0)	{1}	(0)	(1)(1)
{0,1,2}	(0,0,1)	{0,2}	(0,1)	{1}	(0)	(1,2)(1)
{0,1,2,3}	(0,0,1,1)	{0,2}	(0,1)	{1,3}	(0,1)	(1,2)(1,2)
{0,1,3,4}	(0,0,1,2)	{0,4}	(0,2)	{1,3}	(0,1)	(1,3)(1,2)
{0,1,2,4}	(0,0,1,3)	{0,2,4}	(0,1,3)	{1}	(0)	(1,2,3)(1)
{0,1,2,4,6}	(0,0,1,3,4)	{0,2,4,6}	(0,1,3,4)	{1}	(0)	(1,2,3,4)(1)
{0,1,2,6,8}	(0,0,1,3,5)	{0,2,6,8}	(0,1,3,5)	{1}	(0)	(1,2,3,4)(1)
{0,1,2,4,8}	(0,0,1,3,6)	{0,2,4,8}	(0,1,3,6)	{1}	(0)	(1,2,3,4)(1)
{0,1,2,3,4}	(0,0,1,1,3)	{0,2,4}	(0,1,3)	{1,3}	(0,1)	(1,2,3)(1,2)
{0,1,3,4,8}	(0,0,1,2,5)	{0,4,8}	(0,2,5)	{1,3}	(0,1)	(1,3,4)(1,2)
{0,1,2,4,5}	(0,0,1,2,3)	{0,2,4}	(0,1,3)	{1,5}	(0,2)	(1,2,4)(1,3)
{0,1,2,4,9}	(0,0,1,3,3)	{0,2,4}	(0,1,3)	{1,9}	(0,3)	(1,2,3)(1,3)
{0,1,2,4,17}	(0,0,1,3,4)	{0,2,4}	(0,1,3)	{1,17}	(0,4)	(1,2,3)(1,4)

in an orbit of size 1 if all the ϕ_i's and all the $\mathcal{S}_i$'s are equal, in an orbit of size 3 if two of the ϕ_i's and the corresponding two of the $\mathcal{S}_i$'s are equal and in an orbit of size 6 otherwise. There are $N(k)$ pairs of the first type, $3(D(k-1,k-1)N(k)^2 - 3N(k))$ of the second and $D(k-1,k-1,k-1)N(k)^3 - 3(D(k-1,k-1)N(k)^2 - 3N(k)) - N(k)$ of the third. □

This gives the following table of values for $q = 3$ which is sharp for $m \leq 5$:

m	1	2	3	4	5	6
$N(m)$	1	1	2	5	19	≤ 90

A second source of overestimation in Proposition 1.4 stems from the problem of whether or not a given collection of P-ordering equivalence classes for the S_r's will have representatives with P-sequences which realize a specified alignment. The following example shows that this may not always happen.

Proposition 4.8 *For $R = \mathbb{Z}$, $p = 2$ and $m = 8$ there does not exist a 2-ordering equivalence class S with S_0 and S_1 both 2-ordering equivalent to* $\{0, 1, 2, 3\}$ *and alignment* $(1, 2, 3, 4)(1, 2, 3, 5)$.

Proof We first characterize those sequences (d_1, d_2, d_3, d_4) which can arise as 2-sequences of sets 2-order equivalent to $\{0, 1, 2, 3\}$. The subsets S_0, S_1 for $\{0, 1, 2, 3\}$ are $\{0, 2\}$ and $\{1, 3\}$ which both have 2-sequence $(0, 1)$, hence the $(2, 2)$-alignment they determine is $(1, 2)(1, 2)$. If T is any reduced set 2-ordering equivalent to $\{0, 1, 2, 3\}$ then T_0 and T_1 both are of cardinality 2, and so have 2-sequences $(0, a)$ and $(0, b)$ for some $a, b > 0$. Since T is 2-ordering equivalent to $\{0, 1, 2, 3\}$ the union alignment determined by these 2-sequences must be the same as that of $\{0, 1, 2, 3\}$

Table 2

S	D	S_0	D_0	S_1	D_1	S_2	D_2	(ϕ_0, ϕ_1, ϕ_2)
{0}	(0)	{0}	(0)					
{0,1}	(0,0)	{0}	(0)	{1}	(0)			(1)(1)
{0,1,2}	(0,0,0)	{0}	(0)	{1}	(0)	{2}	(0)	(1)(1)(1)
{0,1,3}	(0,0,1)	{0,3}	(0,1)	{1}	(0)			(1,2)(1)
{0,1,3,6}	(0,0,1,2)	{0,3,6}	(0,1,2)	{1}	(0)			(1,2,3)(1)
{0,1,3,9}	(0,0,1,3)	{0,3,9}	(0,1,3)	{1}	(0)			(1,2,3)(1)
{0,1,3,4}	(0,0,1,1)	{0,3}	(0,1)	{1,4}	(0,1)			(1,2)(1,2)
{0,1,4,9}	(0,0,1,2)	{0,9}	(0,2)	{1,4}	(0,1)			(1,3)(1,2)
{0,1,2,3}	(0,0,0,1)	{0,3}	(0,1)	{1}	(0)	{2}	(0)	(1,2)(1)(1)
{0,1,3,9,18}	(0,0,1,3,5)	{0,3,9,18}	(0,1,3,5)	{1}	(0)			(1,2,3,4)(1)
{0,1,3,9,27}	(0,0,1,3,6)	{0,3,9,27}	(0,1,3,6)	{1}	(0)			(1,2,3,4)(1)
{0,1,3,9,12}	(0,0,1,3,4)	{0,3,9,12}	(0,1,3,4)	{1}	(0)			(1,2,3,4)(1)
{0,1,3,12,27}	(0,0,1,3,5)	{0,3,12,27}	(0,1,3,5)	{1}	(0)			(1,2,3,4)(1)
{0,1,3,6,9}	(0,0,1,2,4)	{0,3,6,9}	(0,1,2,4)	{1}	(0)			(1,2,3,4)(1)
{0,1,3,4,6}	(0,0,1,1,2)	{0,3,6}	(0,1,2)	{1,4}	(0,1)			(1,2,3)(1,2)
{0,1,4,9,18}	(0,0,1,2,4)	{0,9,18}	(0,2,4)	{1,4}	(0,1)			(1,3,4)(1,2)
{0,1,9,18,28}	(0,0,2,3,4)	{0,9,18}	(0,2,4)	{1,28}	(0,3)			(1,2,4)(1,3)
{0,1,3,6,10}	(0,0,1,2,2)	{0,3,6}	(0,1,2)	{1,10}	(0,2)			(1,2,3)(1,3)
{0,1,3,6,28}	(0,0,1,2,3)	{0,3,6}	(0,1,2)	{1,28}	(0,3)			(1,2,3)(1,4)
{0,1,3,4,9}	(0,0,1,1,3)	{0,3,9}	(0,1,3)	{1,4}	(0,1)			(1,2,3)(1,2)
{0,1,4,9,27}	(0,0,1,2,5)	{0,9,27}	(0,2,5)	{1,4}	(0,1)			(1,3,4)(1,2)
{0,1,9,27,28}	(0,0,2,3,5)	{0,9,27}	(0,2,5)	{1,28}	(0,3)			(1,2,4)(1,3)
{0,1,3,9,28}	(0,0,1,3,3)	{0,3,9}	(0,1,3)	{1,28}	(0,3)			(1,2,3)(1,3)
{0,1,3,9,82}	(0,0,1,3,4)	{0,3,9}	(0,1,3)	{1,82}	(0,4)			(1,2,3)(1,4)
{0,1,2,3,6}	(0,0,0,1,2)	{0,3,6}	(0,1,2)	{1}	(0)	{2}	(0)	(1,2,3)(1)(1)
{0,1,2,3,9}	(0,0,0,1,3)	{0,3,9}	(0,1,3)	{1}	(0)	{2}	(0)	(1,2,3)(1)(1)
{0,1,2,3,4}	(0,0,0,1,1)	{0,3}	(0,1)	{1,4}	(0,1)	{2}	(0)	(1,2)(1,2)(1)
{0,1,2,4,9}	(0,0,0,1,2)	{0,9}	(0,2)	{1,4}	(0,1)	{2}	(0)	(1,3)(1,2)(1)

which implies $a = b$. The 2-sequence of any set 2-order equivalent to $\{0, 1, 2, 3\}$ therefore must be of the form $(0, c, a + 2c, a + 3c)$ for some $c \geq 0$, i.e. a sequence (d_1, d_2, d_3, d_4) with $d_1 = 0$, $d_2 \geq 0$, $d_3 > 2d_2$ and $d_4 = d_2 + d_3$.

If S is a set with S_0, S_1 both 2-ordering equivalent to $\{0, 1, 2, 3\}$ then its 2-sequence must be a $(4, 4)$-shuffle of two sequences (d_1, d_2, d_3, d_4) and (d'_1, d'_2, d'_3, d'_4) both satisfying the conditions above. If the shuffle projects to the $(4, 4)$-alignment $(1, 2, 3, 4)(1, 2, 3, 5)$ then $d_1 = d'_1$, $d_2 = d'_2$, $d_3 = d'_3$ and $d_4 < d'_4$. This is impossible if $d_4 = d_2 + d_3$ and $d'_4 = d'_2 + d'_3$. □

A consequence of this is that an inductive proof of an exact formula for the number of P-ordering equivalence classes will require a description of the possible P-sequences which can arise for a given P-ordering equivalence class.

Tables 1 and 2 gives lists of representatives of some P-ordering equivalence classes of small size for $R = \mathbb{Z}$. For $p = 2$ and $p = 3$ the table includes representatives of all classes of size ≤ 5. These lists verify the assertions that the tables of bounds for $N(m)$ given above are sharp for $m \leq 5$. Each row in the tables contains a representative of the P-ordering equivalence class, S, its P-sequence, D, The intersections of S with the different modulo P residue classes, S_i for $i = 0, 1$ or $i = 0, 1, 2$, the P-sequences of each S_i, denoted D_i, and the union alignment determined by the D_i's, denoted (ϕ_0, ϕ_1) or (ϕ_0, ϕ_1, ϕ_2). The maps ϕ_i in the alignments are described by listing their values.

References

1. Bhargava, M.: P-orderings and polynomial functions on arbitrary subsets of Dedekind rings. J. Reine Angew. Math. **490**, 101–127 (1997)
2. Bhargava, M.: The factorial function and generalizations. Am. Math. Mon. **107**, 783–799 (2000)
3. Boulanger, J., Chabert, J.-L., Evrard, S., Gerboud, G.: The characteristic sequence of integer-valued polynomials on a subset. Lect. Notes Pure Appl. Math. **205**, 161–174 (1999)
4. Boulanger, J., Chabert, J.-L.: Asymptotic behavior of characteristic sequences of integer-valued polynomials. J. Number Theory **80**, 238–259 (2000)
5. Comtet, L.: Advanced Combinatorics, the Art of Finite and Infinite Expansions. Riedel, Dordrecht (1974)
6. Diaconis, P.: Mathematical developments from the analysis of riffle shuffles. In: L.M.S. Symposium, Groups, Combinatorics, and Geometry, Durham, 2001, pp. 73–97. World Scientific, River Edge (2003)
7. Kaparthi, S., Rao, H.R.: Higher dimensional restricted lattice paths. Discrete Appl. Math. **31**(3), 279–289 (1991)
8. Polya, G.: Uber Ganzwertige Polynome in Algebraischen Zahlkorper. J. Reine Angew. Math. (Crelle) **149**, 97–116 (1919)
9. Torres, A., Cobada, A., Nieto, J.: An exact formula for the number of alignments between two DNA sequences. DNA Seq. **14**, 427–430 (2003)