

The Möbius function of factor order

Anders Björner

Department of Mathematics, Royal Institute of Technology, S-100 44 Stockholm, Sweden

Abstract

Björner, A., The Möbius function of factor order, *Theoretical Computer Science* 117 (1993) 91–98.

Intervals in the factor ordering of a free monoid are investigated. It was shown by Farmer (1982) that such intervals (β, α) are contractible or homotopy spheres in case β is the empty word. We observe here that the same is true in general. This implies that the Möbius function of factor order takes values in $\{0, +1, -1\}$. A recursive rule for this Möbius function is given, which allows efficient computation via the Knuth–Morris–Pratt algorithm.

The Möbius function of subword order was studied in Björner (1990). We give here a simpler proof (a parity-changing involution) for its combinatorial interpretation.

1. Introduction

Let A^* denote the free monoid over an alphabet A . The elements of A^* are finite strings of elements from A called *words*. The *length* $|\alpha|$ of a word $\alpha = a_1 a_2 \dots a_n$ is the number of letters n . There is a unique word $\lambda \in A^*$ of length zero, the *empty word*.

We will say that β is a *factor* of α if $\alpha = \gamma\beta\delta$, for some $\gamma, \delta \in A^*$. Furthermore, β is a *left factor* (or prefix) in α if $\delta = \lambda$ and a *right factor* (or suffix) if $\gamma = \lambda$. The relation of being a factor, written as $\beta \leq \alpha$, gives a partial ordering of A^* . As an ordered set A^* has a unique least element λ , and all maximal chains in an interval $[\beta, \alpha] = \{\gamma \in A^* : \beta \leq \gamma \leq \alpha\}$ have length $l(\beta, \alpha) := |\alpha| - |\beta|$.

Let $\alpha = a_1 a_2 \dots a_n \in A^*$. We say that β is a *subword* of α if $\beta = a_{i_1} a_{i_2} \dots a_{i_k}$ for some sequence $1 \leq i_1 < i_2 < \dots < i_k \leq n$. So, a factor is a particular kind of subword. The subword ordering of A^* is discussed in Section 3. See [10] for further general information concerning words.

To be able to state the rule for computing the Möbius function of factor order we need a few more definitions. Let $\alpha = a_1 a_2 \dots a_n$, $n \geq 2$. Then $i\alpha = a_2 a_3 \dots a_{n-1}$ is the

Correspondence to: A. Björner, Department of Mathematics, Royal Institute of Technology, S-100 44 Stockholm, Sweden.

dominant inner factor in α . All factors of $i\alpha$ are called *inner factors* in α . The *dominant outer factor* $\varphi\alpha$ is the longest $\beta \neq \alpha$ which is both a left factor and a right factor of α (possibly $\varphi\alpha = \lambda$). The word α is *trivial* if $a_1 = a_2 = \dots = a_n$.

As an illustration of these definitions, let $\alpha = aabcabb$. Then $i\alpha = abcab$, $\varphi\alpha = \lambda$, $\varphi i\alpha = ab$. Note that $l(\varphi\alpha, \alpha) = 1$ iff α is trivial, and $l(\varphi\alpha, \alpha) = 2$ iff $\alpha = (ab)^k$ or $\alpha = (ab)^k a$ for some $a, b \in A$.

The Möbius function of a poset with finite intervals $[x, y]$ is the \mathbb{Z} -valued function on intervals recursively defined by

$$\sum_{x \leq z \leq y} \mu(x, z) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x < y. \end{cases}$$

For general information concerning Möbius functions see [12, 13].

Theorem 1.1. *The Möbius function of factor order is, for all $\beta \leq \alpha$ in A^* , given by*

$$\mu(\beta, \alpha) = \begin{cases} \mu(\beta, \varphi\alpha) & \text{if } l(\beta, \alpha) > 2 \text{ and } \beta \leq \varphi\alpha \not\leq i\alpha, \\ 1 & \text{if } l(\beta, \alpha) = 2, \alpha \text{ is nontrivial and } \beta = i\alpha \text{ or } \beta = \varphi\alpha, \\ (-1)^{l(\beta, \alpha)} & \text{if } l(\beta, \alpha) < 2, \\ 0 & \text{in all other cases.} \end{cases}$$

Corollary 1.2. $\mu(\beta, \alpha) \in \{0, +1, -1\}$.

Other classes of posets (actually, lattices) whose Möbius function has the $\{0, +1, -1\}$ property have been studied by Björner [1], Greene [7] and Kahn [8]. Note that factor order is not a lattice.

We exemplify the rule with the following computations using $\alpha = abracadabra$:

$$\begin{aligned} \mu(a, \alpha) &= \mu(a, abra) = \mu(a, a) = 1, \\ \mu(b, \alpha) &= \mu(b, abra) = 0, \\ \mu(br, \alpha) &= \mu(br, abra) = 1, \\ \mu(bra, \alpha) &= \mu(bra, abra) = -1. \end{aligned}$$

The pattern-matching algorithm of Knuth et al. [9] shows that $\beta \leq \alpha$ can be decided in $O(|\alpha|)$ time. Their algorithm contains a preprocessing step which gives a linear-time algorithm for computing $\varphi\alpha$ (for this, see also [10, p. 14]). Hence, Theorem 1.1 shows that $\mu(\beta, \alpha)$ can be computed in quadratic time using these algorithms.

Corollary 1.3. $\mu(\beta, \alpha)$ can be computed in $O(|\alpha|^2)$ steps.

Theorem 1.1 is implied by the next result, which describes the topology of open intervals in factor order up to homotopy type. The proof given in Section 2 is easy to convert to a purely combinatorial proof of Theorem 1.1; see Remark A in Section 4.

From now on we will assume some familiarity with the topology of posets; see e.g. [3] for some background. All topological statements about a poset P will refer to its *order complex*, i.e. the simplicial complex of chains (totally ordered subsets), although stronger statements are possible (see Remark B in Section 4).

Define a function s from the intervals $\beta \leq \alpha$ of factor order to the set $\{-\infty, -2, -1, 0, 1, 2, 3, \dots\}$ by the following recursive rule:

- (i) $l(\beta, \alpha) = 0 \Leftrightarrow s(\beta, \alpha) = -2$,
- (ii) $l(\beta, \alpha) = 1 \Leftrightarrow s(\beta, \alpha) = -1$,
- (iii) $l(\beta, \alpha) = 2 \Rightarrow s(\beta, \alpha) = \begin{cases} 0 & \text{if } \alpha \text{ is nontrivial and } \beta = i\alpha \text{ or } \beta = \varphi\alpha, \\ -\infty & \text{otherwise,} \end{cases}$
- (iv) $l(\beta, \alpha) > 2 \Rightarrow s(\beta, \alpha) = \begin{cases} 2 + s(\beta, \varphi\alpha) & \text{if } \beta \leq \varphi\alpha \not\leq i\alpha, \\ -\infty & \text{otherwise.} \end{cases}$

For instance, using our previous example $\alpha = \text{abracadabra}$ we compute $s(a, \alpha) = 2$, $s(b, \alpha) = -\infty$, $s(br, \alpha) = 2$, $s(bra, \alpha) = 1$.

Theorem 1.4. *For all $\beta < \alpha$ in factor order, the open interval $(\beta, \alpha) = \{\gamma \in A^* : \beta < \gamma < \alpha\}$ has the homotopy type of the $s(\beta, \alpha)$ -dimensional sphere if $s(\beta, \alpha) \geq 0$, and is contractible if $s(\beta, \alpha) = -\infty$.*

For the case when β is the empty word this was shown by Farmer [6], and the proof given in the next section is a rather straightforward extension. Since the Möbius function $\mu(\beta, \alpha)$ is the reduced Euler characteristic of the open interval (β, α) , we deduce the following corollary, of which Theorem 1.1 is a simplified restatement.

Corollary 1.5. *For all $\beta \leq \alpha$ in A^* ,*

$$\mu(\beta, \alpha) = \begin{cases} (-1)^{s(\beta, \alpha)} & \text{if } s(\beta, \alpha) \geq -2, \\ 0 & \text{otherwise.} \end{cases}$$

2. Proofs

The analysis of the structure of lower intervals $[\lambda, \alpha]$ to be given here is implicit in Farmer [6]. The general case will follow by restricting attention to an upper part $[\beta, \alpha]$ of such a lower interval.

For a trivial word $\alpha = aa \dots a$ the lower interval $[\lambda, \alpha]$ is a chain of length $|\alpha|$. If α is nontrivial then it covers exactly two words α' and α'' , the left and right factors of length $|\alpha| - 1$. (Clearly, every nontrivial word covers 2 elements and is covered by $2|A|$ elements.) More generally, we have the following lemma.

Lemma 2.1. *Suppose α is nontrivial. Then $[\lambda, \alpha] = [\lambda, i\alpha] \cup [\varphi\alpha, \alpha]$. Furthermore:*

Case 1: If $\varphi\alpha \not\leq i\alpha$, then $[\lambda, i\alpha] \cap [\varphi\alpha, \alpha] = \emptyset$ and $(\varphi\alpha, \alpha)$ consists of two nonempty disjoint chains with no crosswise relations (see Fig. 1a).

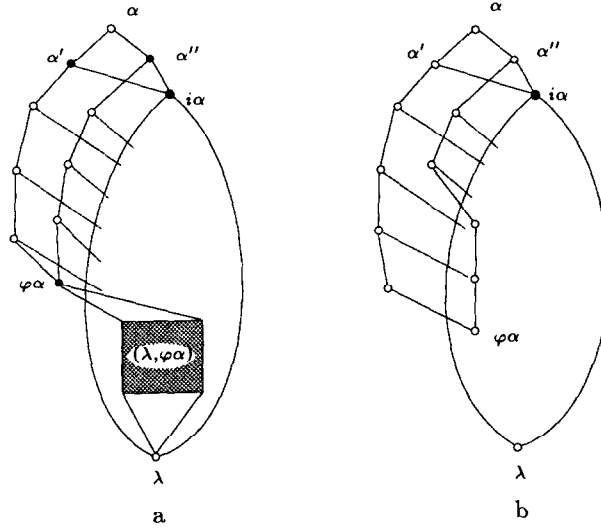


Fig. 1.

Case 2: If $\varphi\alpha \leq i\alpha$, then $(\lambda, \alpha) \setminus (\lambda, i\alpha]$ consists of two nonempty disjoint chains with no crosswise relations (see Fig. 1b).

Proof. Suppose that $\beta \leq \alpha$ is not an inner factor. Then β is a left or right factor in α , let us say a left factor. If $|\beta| < |\varphi\alpha|$, then β is a proper left factor in $\varphi\alpha$, which (using the right factor embedding of $\varphi\alpha$ in α) would make β an inner factor in α . Hence, $|\beta| \geq |\varphi\alpha|$, which implies that $\varphi\alpha \leq \beta$.

Let $\varphi\alpha = \gamma_k < \gamma_{k+1} < \dots < \gamma_{n-1} = a_1 a_2 \dots a_{n-1} = \alpha'$ and $\varphi\alpha = \delta_k < \delta_{k+1} < \dots < \delta_{n-1} = a_2 a_3 \dots a_n = \alpha''$ be the two unique chains of proper left and right factors of $\alpha = a_1 a_2 \dots a_n$ ascending from $\varphi\alpha$, $|\gamma_j| = |\delta_j| = j$. Then the two chains $\gamma_{k+1} < \dots < \gamma_{n-1}$ and $\delta_{k+1} < \dots < \delta_{n-1}$ satisfy the description in case 1. In case 2 one must take the portions of these chains that are outside $[\lambda, i\alpha]$. \square

An element x of a poset P is called *irreducible* if either x is covered by exactly one element or x covers exactly one element. After removing some irreducibles, elements that previously were not irreducible may become so, and conversely. We say that P is *dismantlable* to a subposet Q if Q can be obtained by successive removal of irreducibles from P . This terminology is due to Rival [11]. A poset with a unique least or a unique greatest element (a *cone*) is clearly dismantlable to a point.

Lemma 2.2. Let $\beta < \alpha$, with $l(\beta, \alpha) \geq 3$ and α nontrivial.

Case 1: $\beta \not\leq \varphi\alpha$. Then (β, α) is dismantlable to a point.

Case 2: $\varphi\alpha \leq i\alpha$. Same conclusion as in case 1.

Case 3: $\beta = \varphi\alpha \not\leq i\alpha$. Then (β, α) is dismantlable to the subposet $\{\alpha', \alpha''\}$.

Case 4: $\beta < \varphi\alpha \not\leq i\alpha$. Then (β, α) is dismantlable to the subposet $(\beta, \varphi\alpha) \cup \{\varphi\alpha, i\alpha, \alpha', \alpha''\}$.

Proof. We begin with case 2 (see Fig. 1b). If $\beta \not\leq i\alpha$ then by Lemma 2.1 the interval (β, α) is a chain, and the conclusion is obvious. Suppose that $\beta \leq i\alpha$. From Lemma 2.1 we deduce that $(\beta, \alpha) \setminus (\beta, i\alpha]$ consists of two unrelated chains. These can be removed by deleting irreducible elements from bottom to top. Hence, (β, α) is dismantlable to $(\beta, i\alpha]$, which (being a cone) is further dismantlable to a point.

For the remainder of the proof we assume that $\varphi\alpha \not\leq i\alpha$ (see Fig. 1a). If $\beta \not\leq \varphi\alpha$ (i.e. case 1), then either (i) $\beta > \varphi\alpha$, or (ii) $\beta \in [\lambda, i\alpha] \setminus [\lambda, \varphi\alpha]$. In subcase (i) the interval (β, α) is a chain, and in subcase (ii) one sees from Lemma 2.1 that $(\beta, \alpha) \setminus (\beta, i\alpha]$ consists of two unrelated chains. Hence, in case 1 irreducibles can be removed in exactly the same way as was described for case 2.

Case 3 is easy, since $(\beta, \alpha) = (\varphi\alpha, \alpha)$ consists of two unrelated chains with α' and α'' at the top.

Finally, consider case 4. The elements on the two chains strictly between $\varphi\alpha$ and α', α'' are irreducible and can be removed in any order. After their removal, the maximal elements of $(\beta, i\alpha) \setminus (\beta, \varphi\alpha)$ become irreducible and can be removed. Continuing from top to bottom, all elements of $(\beta, i\alpha) \setminus (\beta, \varphi\alpha)$ eventually become irreducible (being covered only by $i\alpha$) and can successively be removed. At the end of this process only the subposet $(\beta, \varphi\alpha) \cup \{\varphi\alpha, i\alpha, \alpha', \alpha''\}$ remains (see Fig. 2). \square

The *join* of two posets P and Q , denoted as $P * Q$, is the poset on the set $P \cup Q$ in which P and Q retain their internal orders and all elements of P are below all elements of Q . Let A_2 denote the 2-element antichain, and A_2^k the join of k copies of A_2 . (For example, Fig. 2 shows a poset isomorphic to $(\beta, \varphi\alpha) * A_2^2$.)

Lemma 2.3. Suppose that $\beta < \alpha$. If $s(\beta, \alpha) \geq 0$, then (β, α) is dismantlable to a subposet isomorphic to $A_2^{s(\beta, \alpha) + 1}$. If $s(\beta, \alpha) = -\infty$, then (β, α) is dismantlable to a point.

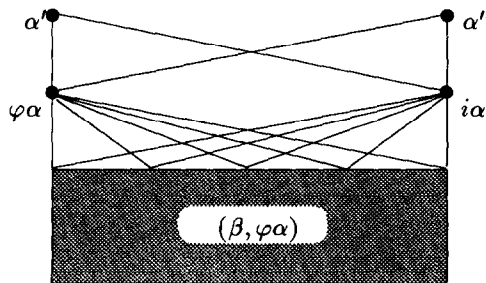


Fig. 2.

Proof. We will use induction on $l(\beta, \alpha) \geq 2$. If $l(\beta, \alpha) = 2$ then (β, α) is either a 2-element antichain or a singleton (since α covers at most 2 elements). These two cases correspond exactly to whether $s(\beta, \alpha) = 0$ or $s(\beta, \alpha) = -\infty$, according to definition (iii) of the function s .

Suppose that $l(\beta, \alpha) > 2$ and that α is not trivial. If $\beta < \varphi\alpha \not\leq i\alpha$ we have by definition (iv) that $s(\beta, \alpha) = s(\beta, \varphi\alpha) + 2$, and Lemma 2.2 shows that (β, α) is dismantlable to a subposet isomorphic to $(\beta, \varphi\alpha) * A_2^2$. By induction, if $s(\beta, \varphi\alpha) \geq 0$ then $(\beta, \varphi\alpha)$ is dismantlable to a subposet isomorphic to $A_2^{s(\beta, \varphi\alpha) + 1}$. It follows that (β, α) is dismantlable to a copy of $A_2^{s(\beta, \varphi\alpha) + 1} * A_2^2 = A_2^{s(\beta, \alpha) + 1}$. If, on the other hand, $s(\beta, \varphi\alpha) = -\infty$ then by induction $(\beta, \varphi\alpha)$ is dismantlable to a point. It follows that (β, α) is dismantlable to a copy of $\{pt\} * A_2^2$, which is further dismantlable to a point (being a cone). The degenerate case when $s(\beta, \varphi\alpha) = -1$, i.e. $l(\beta, \varphi\alpha) = 1$ and $(\beta, \varphi\alpha) = \emptyset$, is easily checked to be consistent.

Keep the assumptions from the preceding paragraph, except let $\beta = \varphi\alpha$. Then $s(\beta, \alpha) = s(\beta, \beta) + 2 = 0$, and by Lemma 2.2 (β, α) is dismantlable to $\{a', \alpha''\} \simeq A_2$.

Suppose now that $l(\beta, \alpha) > 2$, and that α is trivial, or $\beta \not\leq \varphi\alpha$, or $\varphi\alpha \leq i\alpha$. In each of these cases $s(\beta, \alpha) = -\infty$, by definition. If α is trivial then (β, α) is a chain, and hence dismantlable to a point. For the other two cases the conclusion follows from Lemma 2.2. \square

Proof of Theorem 1.4. It is well known, and easy to see, that if x is an irreducible element in a poset P then $P - \{x\}$ is a strong deformation retract of P (the retraction is the simplicial map that sends x to the unique element covering or covered by x and all other elements to themselves; cf. Corollary 10.12 of [3]). Hence, if P is dismantlable to Q then Q is a strong deformation retract of P , and in particular P and Q are homotopy equivalent.

The theorem is therefore a direct consequence of Lemma 2.3. For this, note that the order complex of A_2^{k+1} is homeomorphic to the k -sphere, being the k -fold suspension of the 0-sphere A_2 . \square

3. The Möbius function of subword order

We start with a few definitions. Given a word $\alpha = a_1 a_2 \dots a_n \in A^*$, its *repetition set* is $\mathcal{R}(\alpha) = \{i: a_{i-1} = a_i\} \subseteq \{2, \dots, n\}$. An *embedding* of β in α is a sequence $1 \leq i_1 < i_2 < \dots < i_k \leq n$ such that $\beta = a_{i_1} a_{i_2} \dots a_{i_k}$. It is a *normal embedding* if $\mathcal{R}(\alpha) \subseteq \{i_1, \dots, i_k\}$. For $\alpha, \beta \in A^*$ let

$$\binom{\alpha}{\beta}_n = \text{number of normal embeddings of } \beta \text{ in } \alpha.$$

For instance, $\binom{aabac}{aac}_n = 2$.

The following combinatorial rule for the Möbius function of subword order was given in [2]. The original proof using lexicographic shellability, as well as a later

algebraic proof in [4], is not as simple and elementary as the formula itself. However, both these proofs yield additional information. Here a short and elementary proof (giving no additional information) will be given.

Theorem 3.1. *The Möbius function of subword order is given by*

$$\mu(\beta, \alpha) = (-1)^{|\alpha| + |\beta|} \binom{\alpha}{\beta}_n,$$

for all $\alpha, \beta \in A^*$.

Proof. Suppose that $\gamma \leq \alpha = a_1 a_2 \dots a_n$, and let

$$S = \{1 \leq i_1 < i_2 < \dots < i_k \leq n: \mathcal{R}(\alpha) \subseteq \{i_1, \dots, i_k\} \text{ and } \gamma \leq a_{i_1} \dots a_{i_k}\}.$$

(In this section \leq of course denotes subword order.) Then

$$\sum_{\gamma \leq \beta \leq \alpha} (-1)^{|\alpha| + |\beta|} \binom{\alpha}{\beta}_n = (-1)^n (\#S_{\text{even}} - \#S_{\text{odd}}).$$

Thus, if we show for $\gamma < \alpha$ that S has as many members of even as of odd length (so that the sum equals zero), we will have verified the defining recursion for the Möbius function. To do this we construct a simple parity-changing involution φ on S .

Given $I = (i_1, \dots, i_k) \in S$ let f_I be the minimal number in $\{1, \dots, n\}$ such that f_I is not in the final embedding (j_1, \dots, j_g) of γ in $a_{i_1} \dots a_{i_k}$. The final embedding of γ in δ is the embedding (j_1, \dots, j_g) uniquely characterized by $j'_e \leq j_e$, $1 \leq e \leq g$, for every other embedding (j'_1, \dots, j'_g) of γ in δ . Then define

$$\varphi(I) = \begin{cases} I \cup \{f_I\} & \text{if } f_I \notin I, \\ I - \{f_I\} & \text{if } f_I \in I. \end{cases}$$

It is clear that $\varphi(I) \in S$ in the first case. In the second, i.e. for $f = f_I \in I$, we see that γ is a subword of $a_{i_1} \dots a_{i_k}$ also after a_f is erased (the final embedding remains), and that $\mathcal{R}(\alpha) \subseteq \varphi(I)$ (if $f \in \mathcal{R}(\alpha)$ then $a_{f-1} = a_f$, which is impossible if a_{f-1} but not a_f lies in the final embedding), so that here also $\varphi(I) \in S$.

Along the same lines one sees that $f_{\varphi(I)} = f_I$, because the final embedding of γ remains the same after adding or deleting a_f . This implies that $\varphi^2(I) = I$, for all $I \in S$. \square

As an illustration of the involution φ constructed in the proof, let $\gamma = ab$ and $\alpha = abcab$. Then

$$\begin{array}{ccccccc} . & . & . & a & b & \leftrightarrow & a & . & . & a & b \\ a & . & c & . & b & \leftrightarrow & a & b & c & . & b \\ a & b & . & a & b & \leftrightarrow & . & b & . & a & b \end{array}$$

4. Final remarks

(A) The Möbius number of a poset is the number of odd cardinality chains minus the number of even cardinality chains (see [13, p. 119]). It is easy to see directly that this difference does not change when an irreducible is removed. Therefore, if P is dismantlable to Q it follows that $\mu(P) = \mu(Q)$.

Consequently, Theorem 1.1 can be directly deduced from Lemma 2.3 with no mention of topology. One needs only to check that $\mu(A_2^{k+1}) = (-1)^k$ and $\mu(pt.) = 0$.

(B) If a poset P is dismantlable to a subposet Q , then Q is a strong deformation retract of P in the “ideal topology”, a finite topology studied by Stong [14], Farmer [5] and others. Hence, one can from Lemma 2.3 deduce an “ideal topology” version of Theorem 1.4, which with known implications is strictly stronger than the stated “order complex topology” version. Farmer [6] takes this point of view in his study of the $\beta = \lambda$ case.

(C) Kahn [8] uses the method of “nonevasiveness” to prove that $\mu(x, y) = 0$ in certain posets. It is known that “dismantlable to a point” implies “nonevasive” (see [3]), so Kahn’s method could also be used here.

(D) In [4] it is shown that for subword order the formal power series $\sum_{\beta \leq \alpha} \alpha$ and $\sum_{\beta \leq \alpha} \mu(\beta, \alpha)\alpha$ are rational for all $\beta \in A^*$. For factor order the first series is rational (a finite automaton can recognize the language of all words containing β as a factor), but the rationality of the second series seems doubtful.

References

- [1] A. Björner, Orderings of Coxeter groups, in: C. Greene, ed., *Combinatorics and Algebra*, Contemporary Math., Vol. 34 (Amer. Mathematical Soc., Providence, RI, 1984) 175–195.
- [2] A. Björner, The Möbius function of subword order, in: D. Stanton, ed., *Invariant Theory and Tableaux*, IMA Volumes in Math. and its Applic., Vol. 19 (Springer, Berlin, 1990) 118–124.
- [3] A. Björner, Topological methods, in: R. Graham, M. Grötschel and L. Lovász, eds., *Handbook of Combinatorics* (North-Holland, Amsterdam), to appear.
- [4] A. Björner and C. Reutenauer, Rationality of the Möbius function of subword order, *Theoret. Comput. Sci.* **98** (1992) 53–63.
- [5] F.D. Farmer, The homology of reflexive relations, *Math. Japon.* **20** (1975) 21–28.
- [6] F.D. Farmer, Homotopy spheres in formal language, *Stud. Appl. Math.* **66** (1982) 171–179.
- [7] C. Greene, A class of lattices with Möbius function $\pm 1, 0$, *European J. Combin.* **9** (1988) 225–240.
- [8] J. Kahn, On lattices with Möbius function $\pm 1, 0$, *Discrete Comput. Geom.* **2** (1987) 1–8.
- [9] D.E. Knuth, J.H. Morris and V.R. Pratt, Fast pattern matching in strings, *SIAM J. Comput.* **6** (1977) 323–350.
- [10] M. Lothaire, *Combinatorics on Words* (Addison-Wesley, Reading, MA, 1983).
- [11] I. Rival, A fixed point theorem for finite partially ordered sets, *J. Combin. Theory Ser. A* **21** (1976) 309–319.
- [12] G.-C. Rota, On the foundations of combinatorial theory I. Theory of Möbius functions, *Z. Wahrsch. Verw. Gebiete* **2** (1964) 340–368.
- [13] R.P. Stanley, *Enumerative Combinatorics, Vol. 1* (Wadsworth, Monterey, CA, 1986).
- [14] R.E. Stong, Finite topological spaces, *Trans. Amer. Math. Soc.* **123** (1966) 325–340.