

Chapter 1: Enumerative Combinatorics on Words

Dominique Perrin and Antonio Restivo

<http://www-igm.univ-mlv.fr/~perrin/Recherche/Publications/>

BookChapters/enhandbook.pdf

version of 10 July 2014

Errata and addenda by Darij Grinberg**1. Errata**

The numbering of pages in the following errata matches the numbering of pages on the paper (not the numbering of pages in the PDF file).

I have read this chapter from its beginning to §1.5.2 (except for a few tangential examples and remarks). This part of the chapter should be covered (almost) completely by these errata. My comments on the rest of the chapter are spotty and random.

- **page 7:** “its links with several connexions with” should probably just be “its links with” or “several connexions with”.
- **page 8:** “well-kown” → “well-known”.
- **page 9:** I would put the words “radix order” in italics, since you are just defining this concept here. Also, I would point out that this “radix order” is better known as the length-lexicographic order.
- **page 9:** I would add the following remark: For any $n \geq 0$, the set A^n of n -tuples of elements of A is identified with a subset of A^* (indeed, every n -tuple $(a_1, a_2, \dots, a_n) \in A^n$ is identified with the word $a_1 a_2 \cdots a_n \in A^*$). This explains how “ $X \cap A^n$ ” is to be understood in §1.2.1, and similar expressions elsewhere.
- **page 10:** “the the product” → “that the product”.
- **page 10:** Somewhere here it would be helpful to define the notation X^* . (Namely, if X is a subset of A^* , then X^* denotes the submonoid of A^* generated by X . This is not always a free monoid, so this is not a particular case of the notation A^* defined on page 8.)
- **page 10:** Add a period at the end of the equality (1.2.3).
- **page 11, Example 2:** “and $y \in aD_a^*b$ ” → “and $y \in D_a^*$, so that $d \in aD_a^*b$ ”.
- **page 11, Example 2:** Remove the period at the end of equation (1.2.6) (the sentence does not end here).

- **page 11, Example 2:** Add periods at the end of equation (1.2.7) and at the end of equation (1.2.8).
- **page 12:** Between (1.2.8) and (1.2.9), the " $n4^n$ " should be in parentheses (since both n and 4^n are meant to be part of the denominator).
- **page 12, Example 3:** "The initial edges are indicated with an incoming edge and the terminal ones with with an outgoing edge" \rightarrow "The initial states are indicated with an incoming arrow and the terminal ones with an outgoing arrow". (There are too many mistakes in this sentence to list.)
- **page 13, Example 5:** In the equation " $M = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ ", replace " M " by " M^n ".
- **page 14, proof of Proposition 2:** Replace " $n/d \geq p/d + q/d$ " by " $n/d \geq p/d + q/d - 1$ ".
- **page 14, Example 6:** You write " $x_{n-4}y_{n-3}$ is a prefix of x_{n-3} and thus of x_{n-1} ". The first part of this is wrong ($x_{n-4}y_{n-3}$ is usually too long to be a prefix of x_{n-3}). The second is correct, but needs to be proven. Here is a sketch of the proof:

Forget that we fixed n . First, it is clear that

$$y_{n+1} = x_n y_{n-1} \quad \text{for each } n \geq 4. \quad (1)$$

(Indeed, this follows by removing the last two letters from the equality $x_{n+1} = x_n x_{n-1}$.) Next, we claim that

$$y_{n+1} = x_{n-1} y_n \quad \text{for each } n \geq 3. \quad (2)$$

(*Proof of (2):* We proceed by induction on n . In the case $n = 3$, the equality (2) holds because both y_4 and $x_2 y_3$ equal a . This covers the induction base. For the induction step, we fix an integer $m \geq 4$, and we assume that (2) holds for $n = m - 1$. We must now prove that (2) holds for $n = m$.

We have assumed that (2) holds for $n = m - 1$. In other words, we have $y_m = x_{m-2} y_{m-1}$. But the recursive definition of the Fibonacci sequence of words yields $x_m = x_{m-1} x_{m-2}$. Now, (1) (applied to $n = m$) yields $y_{m+1} = \underbrace{x_m}_{=x_{m-1}x_{m-2}} y_{m-1} = x_{m-1} \underbrace{x_{m-2} y_{m-1}}_{=y_m} = x_{m-1} y_m$. In other words, (2) holds for $n = m$. This completes the induction step. Thus, (2) is proven by induction.)

Now, assume that $n \geq 6$. Then, (2) (applied to $n - 3$ instead of n) yields $y_{n-2} = x_{n-4} y_{n-3}$. Hence, $x_{n-4} y_{n-3}$ is a prefix of x_{n-2} (since y_{n-2} is clearly a prefix of x_{n-2}) and thus also a prefix of x_{n-1} (since $x_{n-1} = x_{n-2} x_{n-3}$). This completes the proof of your claim.

- **page 14, §1.3.1:** You write: "The conjugacy class of a word of length n and period p has p elements if p divides n and has n elements otherwise.". Here you probably mean "minimal period" rather than "period", since otherwise this is clearly false. But I'm not sure how to prove it when p is the minimum period either. (Fortunately you don't actually use this observation; Proposition 3 is clear for simpler reasons.)
- **page 14, §1.3.2:** The notions of a *primitive necklace* (= a necklace consisting of primitive words) and of the *length* of a necklace (= the length of any word in it) should be defined. Also, it should be explained what you mean by "on k letters" (namely, you mean that you are working over a k -letter alphabet A ; you are not requiring that all its k letters are actually being used in the necklace).
- **page 14, §1.3.2:** Add a period after the equality (1.3.11).
- **page 15:** "The Möbius function is defined" \rightarrow "The Möbius function is the function $\mu : \mathbb{N} \setminus 0 \rightarrow \mathbb{Z}$ defined". (Otherwise, the " μ " in the equality is out of place.)
- **page 16:** It makes sense to mention that the convolution product of functions $\mathbb{N} \setminus 0 \rightarrow R$ is commutative whenever R is commutative. (You use this tacitly.)
- **page 16, proof of Proposition 4:** At the very end of the proof, replace " $\sum_{n=de} \mu(d)k^e$ " by " $\sum_{n=de} k^d \mu(e)$ " (this is equivalent, but closer to what you get from the convolution product, and also closer to the expression you want).
- **page 17:** "the set M_d of integers $m \leq n$ " \rightarrow "the set M_d of positive integers $m \leq n$ ".
- **page 17, proof of Proposition 6:** It is not clear what you mean by "the multiset formed by the n circular shifts of the words of length n ". The obvious interpretation would be to consider both the two shifts 12 and 21 of the word 12 and also the two shifts 21 and 12 of the word 21; but this is not what you mean. Instead, the multiset you want is the multiset obtained by picking a representative of each necklace (of length n on k letters), and then writing down all n cyclic shifts of each necklace you have picked. (When the necklace is not primitive, there will be repetitions among its shifts, whence you get a multiset, not a set.)
- **page 17, proof of Proposition 6:** When you defined periods of a word, you required them to be positive integers. Here, you are using 0 as a period of a word. Either this or the definition of a period needs to be modified (although it shouldn't be difficult to do so).

- **page 18, §1.3.3:** "has a unique factorization" → "has at most one factorization".

I would furthermore illustrate this notion of a "factorization" of a necklace by a picture: If we draw out the necklace on a circle, then a factorization means a way of partitioning this circle into arcs (with each arc starting and ending in the middle between two consecutive letters) such that each arc gives a word in X (when you read the letters on this arc in clockwise order). Such factorizations are considered equal when the corresponding arcs are the same (or, more precisely: the points where one arc ends and the next one begins are the same). Thus, $\{aa\}$ is not a circular code (since the necklace corresponding to the word $aaaa$ has two different factorizations; these factorizations are different even though the factors are all the same!), and $\{aba, aabaa\}$ is not a circular code either (since the necklace $baaabaaa$ has two factorizations: either of the two "b"s can be part of an "aba" factor or part of an "aabaa" factor).

- **page 18, §1.3.3:** I think you want to require circular codes to consist of **nonempty** words. Otherwise, the "Formally" version of the definition of a circular code would allow $X = \{\emptyset\}$ (since the condition is vacuously true: s can never be nonempty if $\emptyset = ps$), and then the denominator $1 - f_X(z)$ in (1.3.16) would vanish.
- **page 19:** On the line directly after (1.3.15), replace "in such a way that" by ", so that". See, e.g., this page about "so that" vs. "such that".
- **page 19, Theorem 1.3.1:** "let S be the set of words" → "let S be the set of nonempty words". It is not quite clear whether the empty word counts as being conjugate to itself, but let's avoid this issue altogether by forbidding it. (If you allowed the empty word to be in S , then the left hand side of (1.3.17) would have constant term 1 while the right hand side has constant term 0.)
- **page 19, Theorem 1.3.1:** The period at the end of (1.3.16) should be a comma.
- **page 19, proof of Theorem 1.3.1:** "is of this form for some $x \in X$ " → "is of this form for some unique $x \in X$ ".
- **page 19, proof of Theorem 1.3.1:** "Thus $g_{x,n}$ " → "Thus $g_{n,x}$ ".
- **page 19, proof of Theorem 1.3.1:** "Formula (1.3.16) is obtained from (1.3.17) by taking the derivative of the logarithm of each side" → "Formula (1.3.16) is obtained from (1.3.17) by dividing both sides by z , then taking antiderivatives (with constant term 0) and exponentiating".
- **page 20:** "in such a way that" → ", so that".

- **page 20:** Between the first two paragraphs of this page, I would add the following observation: The set S is not a semigroup, but (due to (1.3.15)) it is closed under taking powers and radicals (i.e., for a word $w \in X^*$ and a positive integer m , we have $w \in S$ if and only if $w^m \in S$). Furthermore, S is closed under cyclic shifting, whence S is a disjoint union of necklaces.
- **page 20:** Replace “and let $p_n = \text{Card}(P \cap A^n)$ ” by “and let p_n be the number of necklaces of length n contained in P ”. (The expression “ $P \cap A^n$ ” is meaningless, since the elements of P are necklaces, not words.)
- **page 20:** Add a period after “Thus $c_n = \sum_{d|n} p_d$ ”.
- **page 22, Proposition 7:** “of its proper suffixes” \rightarrow “of its nonempty proper suffixes”.
- **page 22, proof of Proposition 7:** After “But $uv < tv$ implies $u < t$ ”, add “(because $|u| = |w| - |v| = |t|$)”.
- **page 22, proof of Proposition 8:** Replace “ $m < v$ and thus $\ell m < m < v$ ” by “ $m \leq v$ and thus $\ell m < m \leq v$ ”.
- **page 22, proof of Proposition 8:** After “we have $v = v'm$ ”, add “for some nonempty suffix v' of ℓ ”.
- **page 22, proof of Proposition 8:** After “Then $\ell < v'$ ”, add “(but $|\ell| > |v'|$)”.
- **page 23:** You write: “It motivated Knuth to call Lyndon words *prime* words in [26]”. This is correct, but it is worth mentioning that David Radford already called them “primes” in his 1977 paper *A Natural Ring Basis for the Shuffle Algebra and an Application to Group Schemes* (Journal of Algebra **58** (1979), pp. 432–454), except that he works with the reverse of the lexicographic order on A^* .
- **page 23, proof of Lemma 1:** “let v be the minimal suffix” \rightarrow “let v be the minimal nonempty suffix”.
- **page 23, Proposition 9:** This proposition also easily follows from Exercise 6.1.32 in Darij Grinberg and Victor Reiner, *Hopf Algebras in Combinatorics*, arXiv:1409.8356v5. (Indeed, combining parts (c) and (b) of this exercise yields the implication $\mathcal{F}' \implies \mathcal{G}'$, which shows that each word in P is a sesquipower of a Lyndon word; conversely, if w is a sesquipower of a Lyndon word distinct from the maximal letter, then parts (f) and (b) of the exercise yield the relation $\mathcal{G}' \implies \mathcal{F}'$, which entails that $w \in P$.)

I am mentioning this because the exercise gives a few more equivalent characterizations of P .

- **page 24, proof of Lemma 2:** After the first sentence of this proof, add: "Pick n minimal with this property".
- **page 24, proof of Lemma 2:** How exactly does $x < tar$ yield $q < t$? Couldn't t be a prefix of q ?

I don't know the answer, but here is an alternative way of proving the claim that you are actually trying to prove: We want to show that $qb \in L$. Assume the contrary. Thus, according to the contrapositive of Proposition 7, there exists some nonempty proper suffix of qb that is not larger than qb . Consider this suffix, and observe that it must have the form tb for some proper suffix t of q (since every nonempty proper suffix of qb has this form). Consider this t . Thus, tb is not larger than qb . In other words, $tb \leq qb$. But t is a proper suffix of q , and thus tar is a proper suffix of x (since $x = qar$). By Proposition 7, this implies that $x < tar$ (since x is Lyndon). Thus, $qar = x < tar$. If t is not a prefix of q , then this yields $q < t$ and therefore $qb < tb$ (since q is longer than t and thus cannot be a prefix of t), which contradicts $tb \leq qb$. Thus, t must be a prefix of q . In other words, $q = th$ for some word h . Consider this h . This word h is nonempty (since otherwise, we would have $h = \emptyset$ and thus $q = t \underbrace{h}_{=\emptyset} = t$, which would

contradict the fact that t is a proper suffix of q). We have $tb \leq qb = thb$ (since $q = th$), thus $b \leq hb$. Hence, $b \leq h_1$, where h_1 denotes the first letter of h . (Note that the first letter of h exists, because h is nonempty.) Hence, $a < b \leq h_1$, so that $ar \leq h$ and therefore $tar \leq th = q \leq qar$. This contradicts $qar < tar$. This contradiction shows that our assumption was false. Hence, we have proven that $qb \in L$.

- **page 24, proof of Lemma 2:** "for any $m \geq 1$ " \rightarrow "for any $m \geq 0$ " (in the last sentence of this proof).
- **page 24, proof of Proposition 9:** After "we have $x^n pb \in L$ ", add "(since $x^n pb$ is a prefix of the minimal word $x^n \underbrace{paq}_{=x} = x^{n+1}$)".
- **page 24, proof of Proposition 9:** "then w is is" \rightarrow "then w is".
- **page 24, proof of Proposition 9:** "Finally if $b < a$, w is a Lyndon word by Lemma 2" \rightarrow "Finally, if $b < a$, then w is a Lyndon word by Lemma 2 (applied to v , b and a instead of p , a and b), because vb is a prefix of the minimal word $vbu = y^{n+1}$ ".
- **page 24, §1.4.2:** "an extension" \rightarrow "an n -extension" (you haven't defined the word "extension" on its own).
- **page 26:** "assignement" \rightarrow "assignment".

- **page 26, §1.5:** You use the word "graph" to mean "directed graph". This should probably be explained.
- **page 26, §1.5:** "The de Bruijn graph of orders" → "The de Bruijn graphs of orders".
- **page 26, §1.5:** Your notion of a "cycle" in a graph allows repeated vertices. This being unusual, I suggest you clarify this explicitly. (Normally, this notion is known as "circuit", not as "cycle".)
The same applies to the notion of a "path" (from page 28 onwards). (Your notion of "path" is normally called "walk".)
- **page 27, caption of Figure 1.5.7:** "de Bruin" → "de Bruijn".
- **page 27, proof of Theorem 1.5.1:** How do you know that "Every vertex of H has an indegree equal to its outdegree"? I understand why this would be true for weakly connected components, but why for strictly connected components?
You can fix this problem by replacing "strongly connected" by "weakly connected" (i.e., cannot be written as a union of two vertex-disjoint subgraphs) in Theorem 1.5.1 and throughout its proof.
- **page 27, proof of Theorem 1.5.1:** "Eulerian cycle" → "Euler cycle".
- **page 28:** "and by $d^-(v)$ its outdegree" → "and by $d^+(v)$ its outdegree".
- **page 28:** "A variant of an Euler cycle is that of *Euler path*" → "A variant of an Euler cycle is the notion of an *Euler path*".
- **page 28:** "that a graph" → "that a strongly connected graph".
- **page 28:** After "has an Euler path from x to y ", add "(where x and y are two given distinct vertices)".
- **page 28 and further:** "Eulerian path" → "Euler path" (or vice versa, but consistently).
- **page 28:** In the discussion of the EULER algorithm, it appears that " p " should be " t ".
- **page 28, §1.5.1:** "de Bruin" → "de Bruijn".
- **page 28, §1.5.1:** In the definition of $\pi(G)$, you want G to have at least one outgoing edge from each vertex (so that the factors $(d^+(v) - 1)!$ are well-defined).
- **page 28 and elsewhere:** "van Aarden" → "van Aardenne".

- **page 29, Theorem 1.5.3:** Replace " $t(G)$ " by " $t(v)$ " both times in this theorem. (You use the " $t(v)$ " notation later in the proof, and it is the more reasonable notation, since this value depends on v .)
- **page 29, proof of Theorem 1.5.3:** Replace " φ " by " φ_v " (or vice versa) throughout the proof.
- **page 29, proof of Theorem 1.5.3:** Your claim that "we reach v in a finite number of steps" needs to be proven.

(The proof is not very difficult: If we start at w and keep following T -edges¹ (let us call this the T -walk), then the edges we traverse appear in our Euler path P in the same order as we traverse them in the T -walk (because otherwise, there would be a subpath $p \xrightarrow{a} q \xrightarrow{b} r$ of our T -walk consisting entirely of T -edges such that a appears later than b in the Euler path P ; but this would mean that after traversing a , the Euler path P gets stuck at the vertex q because it has already traversed the last outgoing edge from q (namely, b); but this is clearly absurd since $q \neq v$). Hence, we cannot keep following these edges forever; i.e., our T -walk must end at some vertex. This vertex clearly must be v , since v is the only vertex without an outgoing T -edge. And so we reach v in a finite number of steps.)

- **page 29, proof of Theorem 1.5.3:** Your claim that "There results an Euler path P from v to v which is such that $\varphi(P) = T$ ". This needs to be proven. (Here is how I prove this:

First, let us show that for every vertex $w \neq v$, there exists exactly one T -edge outgoing from w . Indeed, such a T -edge clearly exists (since T is a spanning tree oriented towards v , and therefore each vertex has a path to v). But if there were two distinct T -edges outgoing from the same vertex w , then they could be extended to two different T -paths² from w to v (since T is a spanning tree oriented towards v , and therefore each vertex has a path to v); but the definition of a "spanning tree oriented towards v " shows that there can be only one such a T -path. Hence, for every vertex $w \neq v$, there exists exactly one T -edge outgoing from w . This shows that (for a vertex $w \neq v$) we can speak of "the T -edge outgoing from w " (without having to check that it exists and is unique).

For a similar reason, there cannot be any T -edge outgoing from v (indeed, such a T -edge would start a nontrivial T -path from v to v , but there is also a trivial T -path from v to v , and having two different T -paths from v to v would cause the same contradiction as before).

¹A " T -edge" means an edge that belongs to T .

²A " T -path" means a path that uses only edges from T .

The path P that we build must end at some vertex w (since eventually we run out of unused edges). Consider this w .

Let us first show that $w = v$. Indeed, assume the contrary. Then, the path P has entered w more often than it has exited w ; but this means that there is still at least one outgoing edge from w left unused (because $d^+(w) = d^-(w)$ (since G is Eulerian)). This is absurd, because the path P can only get stuck at a vertex if all outgoing edges from this vertex have been used. This contradiction shows that our assumption was false. Hence, $w = v$ is proven. Thus, P is a path from v to v . Hence, P is a closed path.

Next, we need to show that the path P is an Euler path. Indeed, assume the contrary. Thus, the path P leaves at least one edge of G unused.

Fix a vertex w of G . Then,

$$\begin{aligned}
 & \text{(the number of outgoing edges from } w \text{ unused by } P) \\
 &= \underbrace{\text{(the number of outgoing edges from } w)}_{\substack{=d^+(w)=d^-(w) \\ \text{(since } G \text{ is Eulerian)}}} \\
 &\quad - \underbrace{\text{(the number of outgoing edges from } w \text{ used by } P)}_{\substack{= \text{(the number of incoming edges into } w \text{ used by } P) \\ \text{(since } P \text{ is a closed walk, and thus leaves } w \text{ as often as it enters } w)}} \\
 &= \underbrace{d^-(w)}_{\substack{= \text{(the number of incoming edges into } w)}} \\
 &\quad - \text{(the number of incoming edges into } w \text{ used by } P) \\
 &= \text{(the number of incoming edges into } w) \\
 &\quad - \text{(the number of incoming edges into } w \text{ used by } P) \\
 &= \text{(the number of incoming edges into } w \text{ unused by } P).
 \end{aligned}$$

Hence, there exists an outgoing edge from w unused by P if and only if there exists an incoming edge into w unused by P . In this case, we shall say that the vertex v is *unfulfilled* (by the path P).

Forget that we fixed w . We thus have defined the notion of an "unfulfilled" vertex. At least one vertex of G is unfulfilled (since the path P leaves at least one edge of G unused).

Next, we shall argue that

$$\left(\begin{array}{l} \text{if } p \text{ is an unfulfilled vertex, and if } q \text{ is any vertex} \\ \text{such that there exists a } T\text{-edge from } p \text{ to } q, \\ \text{then } q \text{ is unfulfilled as well} \end{array} \right). \quad (3)$$

[*Proof of (3)*]: Let p be an unfulfilled vertex. Let q be any vertex such that there exists a T -edge from p to q . We must show that q is unfulfilled as well.

The vertex p is unfulfilled. In other words, there exists an outgoing edge from p unused by P (by the definition of "unfulfilled"). Hence, the T -edge outgoing from p is also left unused by P (since P only uses T -edges as a last resort, once all the other outgoing edges are used up). This T -edge must be precisely the T -edge from p to q whose existence we have assumed (because there is only one T -edge outgoing from p). Hence, this T -edge is incoming into q . Thus, there exists an incoming edge into q unused by P . In other words, q is unfulfilled (by the definition of "unfulfilled"). This proves (3).]

Recall that a T -path consists of T -edges. Hence, the following holds:

$$\left(\begin{array}{l} \text{if } p \text{ is an unfulfilled vertex, and if } q \text{ is any vertex} \\ \text{such that there exists a } T\text{-path from } p \text{ to } q, \\ \text{then } q \text{ is unfulfilled as well} \end{array} \right). \quad (4)$$

(Indeed, this can be proven by induction on the length of the T -path, using (3) in the induction step.)

Now, recall that at least one vertex of G is unfulfilled. Pick such a vertex and denote it by p . There exists a T -path from p to v (since T is a spanning tree oriented towards v). Hence, (4) (applied to $q = v$) shows that v is unfulfilled. In other words, there exists an outgoing edge from v unused by P (by the definition of "unfulfilled"). But this contradicts the fact that the path P ends at v (since the path P only ends when it arrives at a vertex whose all outgoing edges are already used). This contradiction shows that our assumption was false. Hence, P is an Euler path.)

- **page 29, proof of Theorem 1.5.3:** " $\pi(v)$ " should be " $\pi(G)$ " at the very end of this proof.
- **page 30:** "Let M be its adjacency matrix defined" \rightarrow "Let M be its adjacency matrix, i.e., the $V \times V$ -matrix defined".
- **page 30:** "Let D be the diagonal matrix" \rightarrow "Let D be the diagonal $V \times V$ -matrix".
- **page 30, Theorem 1.5.4:** Add a period at the end of this theorem.
- **page 30, proof of Theorem 1.5.4:** The induction base (i.e., the case when there are no edges) needs a separate treatment of the case when $V = \{v\}$ (because if $V = \{v\}$, then $N_v(G)$ and $K_v(G)$ are 1, not 0).
- **page 30, proof of Theorem 1.5.4:** The induction step does not work when $w = v$ (that is, when e is a self-loop). Such edges can be dealt with through a much simpler argument, of course (just observe that neither $N_v(G)$ nor $K_v(G)$ changes when a self-loop is removed); but this should be mentioned.

- **page 30, proof of Theorem 1.5.4:** "and G'' the graph obtained by merging v and w " \rightarrow "and G'' the graph obtained from G' by merging v and w ".
I would also explicitly say that all other edges between v and w (apart from e) become self-loops when v and w are merged.
- **page 31, proof of Theorem 1.5.4:** "being the same" \rightarrow "is the same".
- **page 31, proof of Theorem 1.5.4:** Before "By (1.5.22) and (1.5.23)", add a period.
- **page 31, Example 13:** You should probably say that in constructing the matrix L , you have chosen the vertices bb, ba, ab, aa of G to correspond to the rows 1, 2, 3, 4 (and the columns 1, 2, 3, 4) of the matrix L in this order.
- **page 31, Example 13:** Add a period after the displayed equation, and remove the period just before the displayed equation.
- **page 31, Example 13:** "by Example 1.5.8" \rightarrow "by Example 12".
- **page 31:** You should say that "the de Bruijn graph G_n " means the de Bruijn graph of order n on the k -letter alphabet A .
- **page 31:** The sentence "If G is regular, the number $t(G)$ of spanning trees oriented towards a vertex v does not depend on v " is confusing (this has to do with the Eulerianness, not with the regularity, of G). I suggest replacing it by the following:
"If G is Eulerian, then the number $t(v)$ of spanning trees oriented towards a vertex v does not depend on v (since Theorem 1.5.3 shows that it equals the number of Euler cycles of G divided by $\pi(G)$). Thus, we can denote this number by $t(G)$. Hence, in particular, $t(G)$ is defined whenever G is a regular graph (since any regular graph is Eulerian)."
- **page 31, Theorem 1.5.5:** An alternative (combinatorial) proof of this theorem (and actually of a more general result) has been given in: Hoda Bidkhori, Shaunak Kishore, *A Bijective Proof of a Theorem of Knuth*, *Combinatorics, Probability and Computing* **20** (2011), Issue 01, pp. 11–25, Theorem 1.1.
- **page 32, Lemma 3:** "its longest prefix" \rightarrow "the longest prefix of w ". (There are two different words to which the "its" could refer to.)
- **page 32, proof of Lemma 3:** You say that " $wv < sv$ ". This is only true if $s \neq \emptyset$. (Of course, the case when $s = \emptyset$ is easy to deal with, but not in the exact way you are doing it.)

- **page 32, proof of Lemma 3:** I don't understand this proof (starting with the "If $t \leq n - r$ " part). Here is, instead, how I would prove Lemma 3 (not claiming that this is a better proof):

Alternative proof of Lemma 3. The word w belongs to the set P that was defined in §1.4.1 (since it is a prefix of a Lyndon word). Hence, it is a sesquipower of a Lyndon word (by Proposition 9). In other words, there exists a Lyndon word v such that w is a sesquipower of v . We shall prove that $v = \ell$.

Indeed, w is a sesquipower of v . In other words, there exist $n \geq 1$ and a proper prefix p of v such that $w = v^n p$. Consider these n and p . Theorem 1.4.1 shows that the word p factorizes uniquely as a nonincreasing product of Lyndon words. In other words, there exist unique Lyndon words p_1, p_2, \dots, p_k such that $p_1 \geq p_2 \geq \dots \geq p_k$ and $p = p_1 p_2 \dots p_k$. Consider these $p_1 p_2 \dots p_k$. We have $w = \underbrace{v^n}_{n \text{ times}} \underbrace{p}_{=p_1 p_2 \dots p_k} = \underbrace{v v \dots v}_{n \text{ times}} p_1 p_2 \dots p_k$. But

the sequence $\underbrace{v, v, \dots, v}_{n \text{ times}}, p_1, p_2, \dots, p_k$ of Lyndon words is nonincreasing³.

Hence, we can apply Lemma 1 to this sequence instead of ℓ_1, \dots, ℓ_m (since $w = \underbrace{v v \dots v}_{n \text{ times}} p_1 p_2 \dots p_k$). We thus conclude that v is the longest prefix of

w which is a Lyndon word (and that the last word in this sequence is the minimal nonempty suffix of w ; but this is not something we need to know). In other words, v is the longest prefix of w in L . But ℓ , too, is the longest prefix of w in L . Thus, both v and ℓ are defined in the same way. Hence, $v = \ell$. Now, w is a sesquipower of v . In other words, w is a sesquipower of ℓ (since $v = \ell$). Hence, w is the n -extension of ℓ (since w has length ℓ). This proves Lemma 3. ■

- **page 32, proof of Theorem 1.5.6:** You are using the notation λ^* for the Kleene closure $\{\lambda\}^*$ where λ is a single letter. This is worth saying.
- **page 32, proof of Theorem 1.5.6:** It is somewhat confusing to declare u and v separately in each of the three cases (a), (b) and (c). I would find it better to introduce them globally, as follows: The word w can clearly be written as $w = r^d$ for some primitive word r and some positive integer d . Consider these r and d . Write r as $r = uv$ in such a way that $vu \in L$ (this can be done, since every primitive word has exactly one Lyndon word in its necklace). Thus, $vu = \ell_k$ for some k (although you don't seem to call it k in case (b)). Now, the three cases are simply:

³*Proof.* In order to see this, we need to check that $v \geq v \geq \dots \geq v \geq p_1 \geq p_2 \geq \dots \geq p_k$. If $k = 0$, then this is obvious, so let us WLOG assume that $k \neq 0$. Hence, p_1 exists.

We have $p_1 \leq p_1 p_2 \dots p_k = p \leq v$ (since p is a prefix of v), so that $v \geq p_1$. Combining this with $p_1 \geq p_2 \geq \dots \geq p_k$, we find $v \geq p_1 \geq p_2 \geq \dots \geq p_k$, so that $v \geq v \geq \dots \geq v \geq p_1 \geq p_2 \geq \dots \geq p_k$. Qed.

- (a) the case when $d = 1$ and $u \notin z^*$;
- (b) the case when $d = 1$ and $u \in z^*$;
- (c) the case when $d > 1$.

[Note: I still don't understand this proof, so I am not completely sure that this change is the right thing to do.]

- **page 34:** You write: "we denote by X_s the set of words such that no factor has a conjugate in $\{\ell_1, \dots, \ell_s\}$ ". This seems to be a wrong definition of X_s , as it would imply that (for $s \geq 1$) the words in X_s cannot contain the letter a (since such a letter would be a factor conjugate to $a = \ell_1$). Or are you talking of factors in the factorization of Theorem 1.4.1? (Even in this case, I guess you mean "conjugate in $\{\ell_1, \dots, \ell_{s-1}\}$ " rather than "conjugate in $\{\ell_1, \dots, \ell_s\}$ ", though. I don't know for sure since I haven't read Moreno's paper.)
- **page 34 and further:** " $(a_n)_{n \in \mathbb{Z}}$ " should be " $(a_n)_{n \in \mathbb{Z}}$ ".
- **page 34, §1.6:** "It is of course equivalent to ask": Why?
- **page 35, proof of Proposition 11 and further:** " $(a_n)_{n \in \mathbb{Z}}$ " should be " $(a_n)_{n \in \mathbb{Z}}$ ".
- **page 36, Figure 1.6.9:** This figure collides with the header of the page.
- **page 39, Theorem 1.6.2:** Here you seem to be repeating the last paragraph before Example 18 from page 38.
- **page 39, Proposition 16:** "a proper suffix of m " \rightarrow "a proper nonempty suffix of m ".
- **page 39, proof of Proposition 16:** "Let t be a proper suffix" \rightarrow "Let t be a proper nonempty suffix".
- **page 39, proof of Proposition 16:** In Case 1, replace " $\ell^n s$ " by " $\ell^i s$ ".
- **page 39, proof of Proposition 16:** In Case 2, why do we have " $t > \ell^i s$ "?
- **page 39, proof of Proposition 16:** In Case 3, replace "proper suffix" by "proper nonempty suffix".
- **page 42, §1.6:** "are build in this way" \rightarrow "are built in this way".
- **page 42, §1.7:** "Suppose w is" \rightarrow "Suppose $w = a_1 a_2 \cdots a_n$ is". (You later use the notation a_i for the letters of w .)
- **page 43, (1.7.25):** Add a period at the end of this equality.
- **page 43, (1.7.26):** Add a period at the end of this equality.

- **page 43:** "Indeed, $b_{\sigma(i)}$ is the last letter of $w_{\sigma(i)}$ " \rightarrow "Indeed, $b_{\sigma(j)}$ is the last letter of $w_{\sigma(j)}$ ".
- **page 43:** Remove the indentation after (1.7.28).
- **page 44, Remark 1.7.1:** Replace " $\sigma(i) = \pi^{i-1}(1)$ " by " $\sigma(i) = \pi^{i-1}(\sigma(1))$ ".
- **page 47:** When you speak of "the order \preceq_ω ", it is worth pointing out that it is a (total) pre-order, not a (total) order. Indeed, if two words u and v are powers of one and the same word, then $u \preceq_\omega v$ and $v \preceq_\omega u$.
- **page 47:** "multiset of necklaces" \rightarrow "multiset of primitive necklaces".
- **page 47:** " $u^{L \setminus |u|}$ " \rightarrow " $u^{L/|u|}$ ".
- **page 48, Theorem 1.8.1:** Have you really shown that Φ is a bijection? I see at most a proof of the injectivity of Φ here.
- **page 55, Theorem 1.9.4:** Add a period at the end of this equation.
- **page 56:** "By Lemma4" \rightarrow "By Lemma 4".