Accepted Manuscript

Three overlapping squares: The general case characterized & applications

Widmer Bland, W.F. Smyth

PII: S0304-3975(15)00547-2
DOI: http://dx.doi.org/10.1016/j.tcs.2015.06.037
Reference: TCS 10294

To appear in: *Theoretical Computer Science*

Received date: 13 March 2014
Revised date: 15 June 2015
Accepted date: 18 June 2015

Please cite this article in press as: W. Bland, W.F. Smyth, Three overlapping squares: The general case characterized & applications, *Theoret. Comput. Sci.* (2015), http://dx.doi.org/10.1016/j.tcs.2015.06.037

Three Overlapping Squares: The General Case Characterized & Applications

Widmer Bland[1] and W. F. Smyth[1,2]

[1] Algorithms Research Group, Department of Computing & Software
McMaster University, Hamilton, Ontario, Canada L8S 4K1
smyth@mcmaster.ca

[2] School of Engineering & Information Technology
Murdoch University, Murdoch WA 6150, Australia

Abstract. The "Three Squares Lemma" [Crochemore & Rytter, 1995] famously explored the consequences of supposing that three squares occur at the same position in a string; essentially it showed that this phenomenon could not occur unless the longest of the three squares was at least the sum of the lengths of the other two. More recently, several papers [Fan *et al.*, 2006; Simpson, 2007; Kopylova & Smyth, 2012; Franek *et al.*, 2012] have greatly extended this result to a "New Periodicity Lemma" (NPL) by supposing that only two of the squares occur at the same position, with a third occurring in a neighbourhood to the right — in these cases also, similar restrictions apply. In this paper an alternative strategy is proposed: the consequences of having only *two* squares at neighbouring positions are carefully analyzed, and then the observation is made that the analysis applies in a straightforward way (though perhaps with complicated details) to the three neighbouring squares problem in its full generality. We then apply these new insights, first to proofs of the final two remaining unproved subcases (out of a total of 14) of the NPL [Fan *et al.*, 2012], then to an instance of the more general problem.

Keywords: string, word, overlapping squares, repetition, run, maximal periodicity.

1 Introduction

Beginning with the "Three Squares Lemma" of Crochemore & Rytter [9], there has for several years been considerable interest in the limitations that may exist on periodicity in strings. An early survey of this topic by Mignosi & Restivo, with useful suggestions for future research directions, appears as Chapter 8 in [22]. In [9] it was shown that three squares could exist at the same position in a string only if the longest of the three was at least the sum of the lengths of the other two. Over the last decade, a sequence of papers [10, 30, 21, 13] greatly generalized

this result and also made it more precise by considering two squares $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$ at the same position, with however the third square $\boldsymbol{w}^2$ offset a distance $k \geqslant 0$ to the right. First stated and proved as the "New Periodicity Lemma" (NPL) in [10], the main theorem has since been made more specific, with 12 of 14 subcases proved [30, 21, 13] — a main achievement of this paper is to establish the two that remain. Thus the assumption that three neighbouring squares of well-defined size exist within these well-defined bounds has been shown to lead to the conclusion that locally the string breaks down into repetitions of small period. In this paper we begin by proving a lemma that deals in a precise way with just two overlapping squares; we then apply this result to complete the proof of the final two cases of the NPL. We are as a consequence able to characterize the general case of three overlapping squares — no two constrained to begin at the same position — and therefore we can make a start on considering the combinatorial consequences.

Interest has been added to this research by a parallel development over the last dozen years or so: the attempt to specify sharp bounds on the number of maximal periodicities ("runs") that can occur in any string of given length n. Kolpakov & Kucherov [19] showed that the maximum number of runs (usually denoted $\rho(n)$) was linear in n, and moreover they described a linear-time algorithm to compute all the runs in any given string; but their proof was non-constructive — the maximum number of runs was shown to be $\Theta(n)$ but no constant of proportionality was specified. As briefly described in Section 2, the resulting research has led to the conclusion that $\rho(n)$ is at least $0.9445757n$ [31, 20] and no more than $n-1$ [2] — in other words, more or less the string length n. What links these two streams of research is a simple observation:

> If the maximum number of runs over all strings of length n is itself approximately n, then on average there will be about one run starting at each position. Thus, if two runs start at some position, there must be some other position, probably nearby, at which no run can start — "probably nearby" because the interference of overlapping squares typically precludes periodic behaviour at one or more positions within the range of the double periodicity. More generally, determining combinatorial constraints on the occurrence of overlapping squares (runs) may lead to a better characterization of $\rho(n)$.

There is a third avenue of research that relates closely to overlapping squares: the computation of all the runs/repetitions in a given string. At present the only way that this can be done is a form of brute force: global data structures (suffix array, longest common prefix array, Lempel-Ziv decomposition) need to be computed in an extended preprocessing phase, when of course runs are generally a *local* phenomenon. Moreover, it has been shown [26] that the *expected* number of runs in a string is much less than string length: runs generally occur sparsely. A global approach is necessitated by the absence of a detailed understanding of the combinatorics of overlapping occurrences of runs in strings.

In Section 2 terminology, notation and the relevant background are reviewed; Section 3 shows how to express the general case of three overlapping squares,

making use of a careful analysis of two overlapping squares; Section 4 makes use of the new result to prove the two remaining subcases (3 & 7) of the NPL; then in Section 5 a further application to the general case of three overlapping squares is proved; finally, in Section 6 we briefly discuss future research directions.

2 Preliminaries

(Usage generally follows [32].) A ***string*** is a finite sequence of symbols (***letters***) drawn from some finite or infinite set Σ called the ***alphabet***. The alphabet ***size*** is $\sigma = |\Sigma|$. We write a string $\boldsymbol{x}$ in mathbold, and we represent it as an array $\boldsymbol{x}[1..n]$ for some $n \geqslant 0$. We call $n = x$ the ***length*** of $\boldsymbol{x}$. For $x = 0$, $\boldsymbol{x} = \boldsymbol{\varepsilon}$, the ***empty string***.

If $\boldsymbol{x} = \boldsymbol{uvw}$, then $\boldsymbol{u}$ is said to be a ***prefix***, $\boldsymbol{v}$ a ***substring*** (or ***factor***) and $\boldsymbol{w}$ a ***suffix*** of $\boldsymbol{x}$. If $\boldsymbol{x} = \boldsymbol{uv}$, $0 \leqslant u < x$, then $\boldsymbol{vu}$ is said to be the $u^{\boldsymbol{th}}$ ***rotation*** of $\boldsymbol{x}$, written $R_u(\boldsymbol{x})$. If $\boldsymbol{x} = \boldsymbol{uv} = \boldsymbol{wu}$ for $u < x$, then $\boldsymbol{u}$ is a ***border*** of $\boldsymbol{x}$, and $\boldsymbol{x}$ has ***period*** $p = x-u$; that is, for every $i \in 1..u$, $\boldsymbol{x}[i] = \boldsymbol{x}[i+p]$. The string

$$\begin{array}{c} \phantom{\boldsymbol{x} =}\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10 \\ \boldsymbol{x} = a\ b\ a\ a\ b\ a\ b\ a\ a\ b \end{array} \tag{1}$$

has borders $abaab$ and ab, hence corresponding periods 5 and 8, respectively.

If $\boldsymbol{v} = \boldsymbol{x}[i..j]$ has period p, where $v/p \geqslant 2$, and if neither $\boldsymbol{x}[i-1..j]$ nor $\boldsymbol{x}[i..j+1]$ (whenever these are defined) has period p, then the range $i..j$ in $\boldsymbol{x}$ is said to be a ***maximal periodicity*** or ***run*** in $\boldsymbol{x}$ [23]. A run is identified by a 4-tuple (i, p, e, t), where we choose p to be the ***minimum period*** of $\boldsymbol{v}$, $e = \lfloor v/p \rfloor \geqslant 2$ is its ***exponent***, and $t = v \bmod p \in 0..p-1$ is its ***tail***. Then $j = i+pe+(t-1)$. The string (1) has five runs

$$(1,3,2,0),\ (1,5,2,0),\ (3,1,2,0),\ (4,2,2,1),\ (8,1,2,0)$$

corresponding to $(aba)^2, (abaab)^2, a^2, (ab)^2a, a^2$, respectively.

Every run in $\boldsymbol{x}$ determines $t+1$ ***repetitions***,

$$(i,p,e),\ (i+1,p,e),\ldots,(i+t,p,e),$$

where $(i',p,e),\ i \leqslant i' \leqslant i+t$, identifies the substring

$$\boldsymbol{x}[i'..i'+pe-1] = \boldsymbol{x}[i'..i'+p-1]^e.$$

Thus every repetition in $\boldsymbol{x}$ is a subrange of exactly one run in $\boldsymbol{x}$. For example, (1) has six repetitions

$$(1,3,2),\ (1,5,2),\ (3,1,2),\ (4,2,2),\ (5,2,2),\ (8,1,2)$$

corresponding to $(aba)^2, (abaab)^2, a^2, (ab)^2, (ba)^2, a^2$, respectively. Where no ambiguity arises, we will generally refer to runs and repetitions as substrings (for example, $(aba)^2, (ab)^2a$) rather than as ranges in $\boldsymbol{x}$ $(1..6, 4..8)$. If $e = 2$, we say

that the repetition is a ***square***. We say that a square $\boldsymbol{u}^2$ is ***irreducible*** if $\boldsymbol{u}$ is not itself a repetition, ***regular*** if $\boldsymbol{u}$ has no square prefix.

There were three classical algorithms proposed [5, 1, 24] for computing all the repetitions in a string of length n, each executing in $O(n \log n)$ time, asymptotically optimal since the ***Fibonacci string*** $\boldsymbol{f_k}$, defined by

$$\boldsymbol{f_0} = b, \boldsymbol{f_1} = a;\ k \geqslant 2 \Longrightarrow \boldsymbol{f_k} = \boldsymbol{f_{k-1}}\boldsymbol{f_{k-2}},$$

contains $O(f_k \log f_k)$ repetitions [5, 18, 12]. In [23] Main proposed an algorithm to compute all the "leftmost" runs, extended by Kolpakov & Kucherov in [19] to compute all runs. As mentioned in Section 1, this approach makes extensive use of preprocessing, but still executes in linear time, based on a complex proof that the maximum number $\rho(n)$ of runs in any string of length n satisfies

$$\rho(n) \leqslant K_1 n - K_2 \sqrt{n} \log_2 n \tag{2}$$

for some universal positive constants K_1 and K_2. Even though [19] provided computational evidence (up to $n = 60$) that $\rho(n) \leqslant n$, the method of proof allowed no bounds to be placed on K_1 and K_2. Over the last decade, the bounding of $\rho(n)/n$ has become a growth industry, leading to a lower bound 0.9445757 [15, 14, 25, 31, 20] and an asymptotic upper bound 1.029 [28, 27, 6, 16, 17, 7, 8], the latter result achieved using three years of CPU time on a supercomputer [29]. Very recently, Bannai *et al.* [2] have published a remarkably simple proof, using Lyndon words, that in fact $\rho(n)/n < 1$ for all n. Meanwhile, more efficient and truly linear (independent of alphabet size σ) algorithms for computing runs have been proposed — for example, [3, 4] — but still with heavy preprocessing and the same general approach. Since, as noted in Section 1, runs are expected to be sparse in strings, even for small σ [26], a heavy-handed global approach seems inappropriate.

A parallel approach has sought to find a combinatorial basis for estimating the maximum number of runs in a string, specifically by considering the consequences of assuming that two squares occur at the same position in a string, with a third nearby, somewhat to the right. This generalizes the "Three Squares Lemma" [9] that considers three squares at the same position in the string:

Lemma 1. *Suppose $\boldsymbol{u}^2$ is irreducible, and suppose $\boldsymbol{v} \neq \boldsymbol{u}^j$ for any $j \geqslant 1$. If $\boldsymbol{u}^2$ is a prefix of $\boldsymbol{v}^2$, in turn a proper prefix of $\boldsymbol{w}^2$, then $w \geqslant u+v$.*

Here is the original NPL, as stated and proved in [10]:

Lemma 2. *If $\boldsymbol{x}$ has regular prefix $\boldsymbol{u}^2$ and irreducible prefix $\boldsymbol{v}^2$, $u < v < 2u$, then for every $k \in 0..v-u-1$ and every $w \in v-u+1..v-1$, $w \neq u$, $\boldsymbol{x}[k+1..k+2w]$ is not a square.*

The proof required consideration of 14 subcases based on the magnitudes of k and w (see Table 1), each of which led to a proof by contradiction of the regularity of $\boldsymbol{u}$. Figure 1 shows two of these subcases.

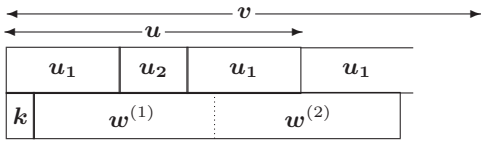


Fig. 1. Subcases 1 & 2 of Lemma 2

Subsequent work has split the range $u < v < 2u$ into two sections $(u, 3u/2]$ and $(3u/2, 2u)$, while eliminating the regularity condition altogether, as we now describe.

In [21] it was shown that for $u < v \leqslant 3u/2$, the requirement that $\boldsymbol{x} = \boldsymbol{v}^2$ with prefix $\boldsymbol{u}^2$ necessitates

$$\boldsymbol{x} = \boldsymbol{t_1}^m \boldsymbol{t_2} \boldsymbol{t_1}^{m+1} \boldsymbol{t_2} \boldsymbol{t_1}, \tag{3}$$

where $t_1 = v-u,\ t_2 = u \bmod t_1,\ m = \lfloor u/t_1 \rfloor \geqslant 2$ and $\boldsymbol{t_2}$ is a proper prefix of $\boldsymbol{t_1}$. It was shown further that, except for $m+5$ precisely identified runs that always occur in $\boldsymbol{x}$, there could be no other runs of period greater than t_1. Thus for $u < v \leqslant 3u/2$, the structure of $\boldsymbol{x}$ is well defined, even without reference to $\boldsymbol{w}$.

Table 1. The 14 subcases identified in [10], slightly modified, for three neighbouring squares $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ (with $v-u < w < v,\ w \neq u,\ 0 \leqslant k < v-u$).

Subcase S	k	$k+w$	$k+2w$	Special Conditions
1	$0 \leqslant k \leqslant u_1$	$k+w \leqslant u$	$k+2w \leqslant u+u_1$	$k \geqslant u_2$
2	$0 \leqslant k \leqslant u_1$	$k+w \leqslant u$	$k+2w \leqslant u+u_1$	$k < u_2$
3	$0 \leqslant k \leqslant u_1$	$k+w \leqslant u$	$k+2w > u+u_1$	—
4	$0 \leqslant k \leqslant u_1$	$u < k+w \leqslant u+u_1$	—	—
5	$0 \leqslant k \leqslant u_1$	$u+u_1 < k+w \leqslant v$	—	—
6	$0 \leqslant k \leqslant u_1$	$v < k+w < 2u$	—	—
7	$u_1 < k < u_1+u_2$	$k+w \leqslant u+u_1$	$k+2w \leqslant 2u$	—
8	$u_1 < k < u_1+u_2$	$k+w \leqslant u+u_1$	$k+2w > 2u$	—
9	$u_1 < k < u_1+u_2$	$u+u_1 < k+w \leqslant v$	—	$w < u$
10	$u_1 < k < u_1+u_2$	$k+w \leqslant v$	$k+2w \leqslant u+v$	$w > u$
11	$u_1 < k < u_1+u_2$	$k+w \leqslant v$	$u+v < k+2w \leqslant 2v-u_2$	—
12	$u_1 < k < u_1+u_2$	$k+w \leqslant v$	$2v-u_2 < k+2w$	—
13	$u_1 < k < u_1+u_2$	$v < k+w \leqslant 2u$	—	—
14	$u_1 < k < u_1+u_2$	$2u < k+w < 2u+u_2-1$	—	—

On the other hand, for $3u/2 < v < 2u$, there is a different breakdown

$$\boldsymbol{x} = \boldsymbol{u_1 u_2 u_1 u_1 u_2 u_1 u_2 u_1 u_1 u_2}, \tag{4}$$

where $\boldsymbol{u} = \boldsymbol{u_1 u_2 u_1},\ \boldsymbol{v} = \boldsymbol{u_1 u_2 u_1 u_1 u_2}$ and $u_1 = 2u-v,\ u_2 = 2v-3u$. Note that setting $\boldsymbol{t_1} = \boldsymbol{u_1 u_2},\ \boldsymbol{t_2} = \boldsymbol{u_1}$ converts the form (4) into (3), but with $m < 2$. For

Table 2. Structure of $\boldsymbol{x}$ for subcases $S \in 1..14$: σ is the largest alphabet size consistent with u, v, k, w [13]; $\boldsymbol{d}$, $\boldsymbol{d_1}$ and $\boldsymbol{d_3}$ are prefixes of $\boldsymbol{x}$ with $d = \gcd(u, v, w)$, $d_1 = \gcd(u-w, v-u)$, $d_2 = \gcd(u, v-w)$, $d_3 = v \bmod d_2$.

Subcases S	Conditions	Breakdown of $\boldsymbol{x}$
$1, 2, 5, 6, 8$–10	$(\forall \boldsymbol{x}, \sigma = d)$	$\boldsymbol{x} = \boldsymbol{d}^{x/d}$
$3, 4, 7$	$(\forall \boldsymbol{x})$	$\boldsymbol{x} = \boldsymbol{d_1}^{u/d_1} \boldsymbol{d_1}^{v/d_1} \boldsymbol{d_1}^{(v-u)/d_1}$
	specified cases	$\boldsymbol{x} = \boldsymbol{d}^{x/d}$
11–14	$\sigma = d$ or $d_2 \leqslant 2u-v$	$\boldsymbol{x} = \boldsymbol{d}^{x/d}$
	otherwise	$\boldsymbol{x} = \left(\left(\boldsymbol{d_3}^{d_2/d_3}\right)^{v/d_2}\right)^2$

this case, after much experimental and theoretical work [30, 21, 13], the revised NPL can be stated as follows:

Lemma 3. *Suppose that a string $\boldsymbol{x}$ has prefixes $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$, $3u/2 < v < 2u$, and suppose further that a third square $\boldsymbol{w}^2$ occurs at position $k+1$ of $\boldsymbol{x}$, where $v-u < w < v$, $w \neq u$, and $0 \leqslant k < v-u$. Then for each of the 14 subcases S identified in Table 1, the corresponding structure of $\boldsymbol{x}$ is given in Table 2.*

In other words, $\boldsymbol{x}$ breaks down into repetitions of small period — essentially, the postulate of three such squares cannot be satisfied. Twelve of the 14 subcases have been proved [30, 21, 13]; in this paper we prove the remaining two, subcases 3 and 7.

We believe moreover that further generalization is of interest: what happens when the three squares $\boldsymbol{u}^2, \boldsymbol{v}^2, \boldsymbol{w}^2$ are merely constrained to be "neighbouring", without the requirement that $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$ occur at the same position? What is an appropriate formulation of such a problem? What relative values of k, u, v, w are of combinatorial interest?

In this paper we begin to answer these questions by first considering only two overlapping squares in some detail, then making the observation that three overlapping squares can always be thought of as two sets of two overlapping squares. In Section 3 a general lemma for two squares is stated and proved, a result used to establish subcases 3 and 7 in Section 4. As a further application, a "sample" three squares lemma is proved in Section 5. Section 6 briefly discusses future work.

We conclude this section by stating results that will be useful in what follows:

Lemma 4. ("The Periodicity Lemma" [11]) *Let p and q be two periods of $\boldsymbol{x} = \boldsymbol{x}[1..n]$, and let $d = \gcd(p, q)$. If $p+q \leqslant n+d$, then d is also a period of $\boldsymbol{x}$.*

Lemma 5. (Corollary to Lemma 4.) *If $\boldsymbol{x} = \boldsymbol{uvw}$, where $\boldsymbol{uv}$ and $\boldsymbol{vw}$ have period $p \leqslant v$, then $\boldsymbol{x}$ has period p.*

Lemma 6. ([22], Lemma 8.1.3) *If a string $\boldsymbol{x}$ of period p has a substring $\boldsymbol{u}$, $u \geqslant p$, of period q, where $q \mid p$, then $\boldsymbol{x}$ has period q.*

Lemma 7. ([21], Lemma 8) *Suppose both* $\boldsymbol{x}$ *and* $R_v(\boldsymbol{x})$, $0 < v < x$, *have period* u, *and let* $\ell = x \bmod u > 0$ *and* $r = \lfloor x/u \rfloor$. *Let* $\boldsymbol{x}_v$ *denote* $R_v(\boldsymbol{x})$, *and let* $d = \gcd(u, \ell)$. *Then*

(a) *if* $r = 1$ *and* $v \geqslant \ell$, $\boldsymbol{x}_{v-\ell}[1..2\ell]$ *is a square of period* ℓ;
(b) *if* $r = 1$ *and* $v \leqslant \ell$, $\boldsymbol{x}[1..v+\ell]$ *has period* ℓ;
(c) *if* $r > 1$ *and* $v < u$, $\boldsymbol{x}[1..v+\ell]$ *has period* ℓ; *if moreover* $v+d \geqslant u$, *then* $\boldsymbol{x}$ *is a repetition of period* d;
(d) *if* $r > 1$ *and* $u \leqslant v \leqslant x-u$, $\boldsymbol{x}[1..u+\ell]$, *hence* $\boldsymbol{x}$, *is a repetition of period* d;
(e) *if* $r > 1$ *and* $x-u < v$, *where* $v' = v-(x-u)$, $\boldsymbol{x}[v'+1..u+\ell]$ *has period* ℓ; *if moreover* $v' \leqslant d$, *then* $\boldsymbol{x}$ *is a repetition of period* d.

Proof (Lemma 7(a)). Let $\boldsymbol{v} = \boldsymbol{x}[1..v] = \boldsymbol{x}_v[x-v+1..x]$, and let $\boldsymbol{u} = \boldsymbol{x}_v[1..u]$, as shown in Figure 2. Since $\boldsymbol{x}_v$ has period u and $v \geqslant \ell$, $\boldsymbol{u}[1..\ell]$ is a suffix of $\boldsymbol{x}_v$ and $\boldsymbol{v}$. Recalling that $\boldsymbol{v}$ is also a prefix of $\boldsymbol{x}$, we see that $\boldsymbol{x}_{v-\ell} = \boldsymbol{v}[v-\ell+1..v]\boldsymbol{u}$ has prefix $(\boldsymbol{u}[1..\ell])^2$. □

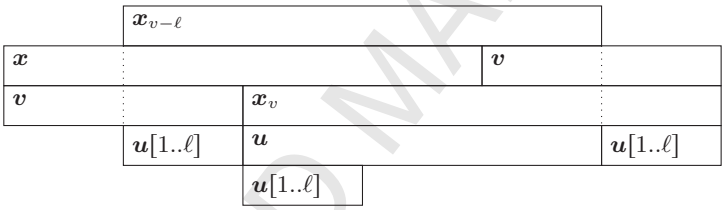


Fig. 2. Lemma 7(a)

3 Characterizing the General Case

We are interested in the cases that arise when a square $\boldsymbol{u}^2$ beginning at some position i in a string overlaps with a second square $\boldsymbol{v}^2$ at position $i+k$, $k \geqslant 0$, to its right.

Lemma 8. *Suppose* $\boldsymbol{x}$ *has prefixes* $\boldsymbol{u}^2$ *and* $\boldsymbol{k}\boldsymbol{v}^2$, $k \geqslant 0$, *where* $x = \max(2u, k+2v)$, $k \leqslant u < 2v$.

(a) $k+v < u < 2v$ $(k < \min(v-1, u-v))$:

$$\boldsymbol{x} = (\boldsymbol{p}^e\boldsymbol{z})^2 = \boldsymbol{p}^e\boldsymbol{q}^f\boldsymbol{q}^{f-e} = \boldsymbol{p}^e\boldsymbol{q}^f\boldsymbol{p}[k+1..u-v],$$

where $\boldsymbol{p} = \boldsymbol{u}[1..u-v]$, $e = \frac{k+v}{u-v} > 1$, $\boldsymbol{z} = \boldsymbol{v}[1..u-(k+v)]$, $\boldsymbol{q} = R_k(\boldsymbol{p})$, $f = \frac{u}{u-v} > 2$, $f-e \leqslant 1$.

(b) $\frac{k}{2}+v \leqslant u \leqslant k+v$ $(1 \leqslant u-v \leqslant k \leqslant 2(u-v))$:

$$\boldsymbol{x} = (\boldsymbol{z}\boldsymbol{p}^e)^2 = (\boldsymbol{q}[1..k+v-u]\boldsymbol{p}^e)^2 = (\boldsymbol{k}\boldsymbol{p}^{e-1})^2,$$

where $\boldsymbol{z} = \boldsymbol{u}[1..k+v-u]$, $\boldsymbol{p} = \boldsymbol{v}[1..u-v]$, $e = 1+\frac{u-k}{u-v} \geqslant 1$, $\boldsymbol{q} = R_c(\boldsymbol{p})$, $c = (u-k) \bmod (u-v)$.

(c) $v < u < \frac{k}{2}+v$ $(k > 2(u-v))$:

$$\boldsymbol{x} = (\boldsymbol{q}\boldsymbol{y}\boldsymbol{p}^e)^2\boldsymbol{y},$$

where $\boldsymbol{p} = \boldsymbol{v}[1..u-v]$, $e = 1+\frac{u-k}{u-v} > 1$, $\boldsymbol{q} = R_c(\boldsymbol{p})$, $c = (u-k) \bmod (u-v)$, $\boldsymbol{y} = \boldsymbol{v}[2u-(k+v)+1..v]$. *Moreover, both* $\boldsymbol{x}$ *and* $\boldsymbol{k}\boldsymbol{v}$ *have border* $\boldsymbol{q}\boldsymbol{y}$.

(d) $v = u$ $(k \geqslant 0)$:

$$\boldsymbol{v} = R_k(\boldsymbol{u}).$$

(e) $\frac{2(k+v)}{3} \leqslant u < v$ $(k \leqslant \frac{3u}{2}-v < \frac{v}{2})$:

$$\boldsymbol{x} = (\boldsymbol{k}\boldsymbol{p}^e)^2\boldsymbol{q}\boldsymbol{k}\boldsymbol{p},$$

where $\boldsymbol{p} = \boldsymbol{v}[1..v-u]$, $e = \frac{u-k}{v-u} > 1$, $\boldsymbol{q} = R_c(\boldsymbol{p})$, $c = (u-k) \bmod (v-u)$. *Both* $\boldsymbol{x}$ *and* $\boldsymbol{k}\boldsymbol{v}$ *have border* $\boldsymbol{k}\boldsymbol{p}$.

(f) $\frac{k+v}{2} < u < \frac{2(k+v)}{3} < v$ $(\frac{3u-2v}{2} < k < 2u-v < u)$:

$$\boldsymbol{x} = \boldsymbol{k}(\boldsymbol{p}^e\boldsymbol{k}\boldsymbol{p})^2,$$

where $\boldsymbol{p} = \boldsymbol{v}[1..v-u]$, $e = \frac{u-k}{v-u} > 1$.

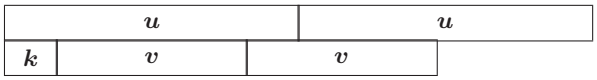
(g) $k \leqslant u \leqslant \frac{k+v}{2}$ ($\boldsymbol{u}^2$ *a prefix of* $\boldsymbol{k}\boldsymbol{v}$) :

$$\boldsymbol{x} = \boldsymbol{k}(\boldsymbol{p}^e\boldsymbol{z})^2,$$

where $\boldsymbol{p} = \boldsymbol{u}[k+1..u]\boldsymbol{u}[1..k]$, $e = \frac{2u-k}{u} \geqslant 1$, $\boldsymbol{z} = \boldsymbol{v}[2u-k+1..v]$.

Proof.

(a) Let $\boldsymbol{z} = \boldsymbol{u}[k+v+1..u] = \boldsymbol{v}[1..u-(k+v)]$, suffix of $\boldsymbol{u}$ and prefix of $\boldsymbol{v}$.



Observe that

$$\boldsymbol{u}[k+j] = \boldsymbol{v}[j] = \boldsymbol{u}[j-z],\ z+1 \leqslant j \leqslant v,$$

so that $\boldsymbol{u}[1..k{+}v] = \boldsymbol{kv}$ has period $k{+}z = u{-}v = p$ (where $\boldsymbol{p} = \boldsymbol{u}[1..u{-}v]$). Consequently, we may write $\boldsymbol{x} = (\boldsymbol{p}^e\boldsymbol{z})^2$, where $e = \frac{k+v}{u-v} > 1$ (since $k{+}v < u$).

Noting that $\boldsymbol{v} = \boldsymbol{u}[k{+}1..u{-}z]$, with $k < u{-}v$, we see also that $\boldsymbol{u} = \boldsymbol{k}\boldsymbol{q}^{f-1}\boldsymbol{z}$, where $\boldsymbol{q} = R_k(\boldsymbol{p})$,

$$f = \frac{u}{u-v} = \frac{v}{u-v}{+}1 > 2.$$

Hence $\boldsymbol{x} = \boldsymbol{p}^e\boldsymbol{z}\boldsymbol{k}\boldsymbol{q}^{f-1}\boldsymbol{z}$. But $\boldsymbol{zk}$ is a prefix of the second copy of $\boldsymbol{v}$ of length p, and comparing with the first copy of $\boldsymbol{v}$, we see that therefore $\boldsymbol{zk} = R_k(\boldsymbol{p}) = \boldsymbol{q}$. Since moreover $\boldsymbol{z} = \boldsymbol{q}^g$, where

$$g = \frac{z}{u-v} = \frac{u}{u-v} - \frac{k+v}{u-v} = f{-}e \leqslant 1,$$

we find $\boldsymbol{x} = \boldsymbol{p}^e\boldsymbol{q}^f\boldsymbol{q}^{f-e}$, as claimed. (Note that $g = 1$ iff $k = 0$.) Finally, writing $\boldsymbol{q} = \boldsymbol{p}[k{+}1..u{-}v]\boldsymbol{p}[1..k]$ and $f{-}e = 1{-}\frac{k}{u-v}$, we find that $\boldsymbol{q}^{f-e} = \boldsymbol{p}[k{+}1..u{-}v]$.

(b) Let $\boldsymbol{z} = \boldsymbol{u}[1..k{+}v{-}u]$, a possibly empty prefix of $\boldsymbol{u}$ and suffix of $\boldsymbol{v}$.

Observe that

$$\boldsymbol{u}[k{+}j] = \boldsymbol{v}[j] = \boldsymbol{u}[z{+}j],\ 1 \leqslant j \leqslant v{-}z = u{-}k,$$

where $z = k{+}v{-}u < k$. Thus $\boldsymbol{u}[z{+}1..u]$ and $\boldsymbol{v}$ have period $k{-}z = u{-}v = p$. Consequently, setting $\boldsymbol{p} = \boldsymbol{u}[z{+}1..k] = \boldsymbol{v}[1..k{-}z]$, we may write $\boldsymbol{x} = (\boldsymbol{z}\boldsymbol{p}^e)^2$, where $e = \frac{u-z}{u-v} \geqslant 1$, since $z \leqslant v$. Noting that

$$u{-}z = u{-}k{-}v{+}u = (u{-}v){+}(u{-}k), \tag{5}$$

we see that $e = 1{+}\frac{u-k}{u-v}$.

Since $\boldsymbol{p}$ is a prefix of $\boldsymbol{v}$ and $z{+}p = k$, it follows that $\boldsymbol{k} = \boldsymbol{zp}$. Thus we can also write $\boldsymbol{x} = (\boldsymbol{k}\boldsymbol{p}^{e-1})^2$.

Finally, setting $\boldsymbol{y} = \boldsymbol{u}[k{+}2v{-}u{+}1..u]$, since $\boldsymbol{zy}$ is a suffix of $\boldsymbol{u}$ of length

$$k{+}v{-}u{+}2(u{-}v){-}k = u{-}v = p,$$

it follows that $\boldsymbol{zy}$ is a rotation of $\boldsymbol{p}$. In fact, $\boldsymbol{zy} = \boldsymbol{q} = R_c(\boldsymbol{p})$, where by (5)

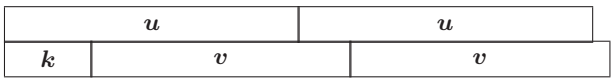
$$c = (u{-}z) \bmod (u{-}v) = (u{-}k) \bmod (u{-}v).$$

Then $\boldsymbol{z} = \boldsymbol{q}^f$, where

$$f = \frac{z}{p} = \frac{(k{+}v){-}u}{u-v} = \frac{k}{u-v}{-}1 \leqslant 1,$$

so that $\boldsymbol{q}^f = \boldsymbol{q}[1..z]$ and $\boldsymbol{x} = (\boldsymbol{q}[1..k{+}v{-}u]\boldsymbol{p}^e)^2$, as required.

(c) Let $\boldsymbol{z} = \boldsymbol{u}[1..k{+}v{-}u]$, nonempty prefix of $\boldsymbol{u}$ and suffix of $\boldsymbol{v}$.



As in (b), observe that

$$\boldsymbol{u}[k{+}j] = \boldsymbol{v}[j] = \boldsymbol{u}[z{+}j],\ 1 \leqslant j \leqslant v{-}z = u{-}k,$$

with $z = k{+}v{-}u < k$. Again $\boldsymbol{u}[z{+}1..u]$ has period $k{-}z = u{-}v = p$, where $\boldsymbol{p} = \boldsymbol{u}[z{+}1..k] = \boldsymbol{v}[1..u{-}v]$. However, unlike (b), not $\boldsymbol{v}$, but only $\boldsymbol{v}[1..v{-}y]$, has period p, where $\boldsymbol{y} = \boldsymbol{v}[2u{-}(k{+}v){+}1..v] = \boldsymbol{v}[u{-}z{+}1..v]$ and

$$y = k{+}2v{-}2u = z{-}(u{-}v) = z{-}p < z.$$

Thus, noting that $z < v$ and setting

$$e = \frac{u{-}z}{u{-}v} = \frac{(u{-}v){+}(u{-}k)}{u{-}v} = 1{+}\frac{u{-}k}{u{-}v} > 1,$$

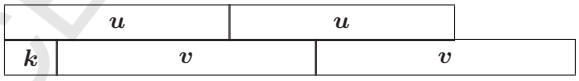
we can write $\boldsymbol{x} = (\boldsymbol{z}\boldsymbol{p}^e)^2\boldsymbol{y}$. Since $\boldsymbol{u}[z{+}1..u]$ has prefix $\boldsymbol{p}$ and $k = z{+}p$, we see that $\boldsymbol{k} = \boldsymbol{z}\boldsymbol{p}$; further, since $\boldsymbol{z}$ has suffix $\boldsymbol{y}$ and $z = p{+}y$, it follows that $\boldsymbol{z} = \boldsymbol{q}\boldsymbol{y}$ for some rotation $\boldsymbol{q}$ of $\boldsymbol{p}$. In fact, $\boldsymbol{q} = R_c(\boldsymbol{p})$, where

$$c = (v{-}y) \bmod (u{-}v) = ((v{-}z){+}(u{-}v)) \bmod (u{-}v) = (u{-}k) \bmod (u{-}v).$$

Noting that $\boldsymbol{k} = \boldsymbol{q}\boldsymbol{y}\boldsymbol{p}$, we see that both $\boldsymbol{k}\boldsymbol{v}$ and $\boldsymbol{x}$ have border $\boldsymbol{q}\boldsymbol{y}$, while $\boldsymbol{x} = (\boldsymbol{q}\boldsymbol{y}\boldsymbol{p}^e)^2\boldsymbol{y}$, as required.

(d) Obvious.

(e) Again let $\boldsymbol{z} = \boldsymbol{u}[1..k{+}v{-}u]$, nonempty prefix of $\boldsymbol{u}$ and suffix of $\boldsymbol{v}$.



Observe that

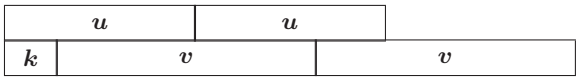
$$\boldsymbol{u}[k{+}j] = \boldsymbol{v}[j] = \boldsymbol{u}[z{+}j],\ 1 \leqslant j \leqslant u{-}z,$$

where $z = k{+}v{-}u > k$. Thus $\boldsymbol{u}[k{+}1..u]$ and $\boldsymbol{v}[1..u{-}k]$ have period $z{-}k = v{-}u = p$. Therefore, setting $\boldsymbol{p} = \boldsymbol{v}[1..z{-}k]$, $e = \frac{u-k}{v-u}$, we can write $\boldsymbol{x} = (\boldsymbol{k}\boldsymbol{p}^e)^2\boldsymbol{y}$, where $\boldsymbol{y} = \boldsymbol{v}[2u{-}(k{+}v){+}1..v]$ is a suffix of $\boldsymbol{v}$, $y = (k{+}v{-}u){+}(v{-}u) = z{+}p > z$. Since $\boldsymbol{z}$ is a suffix of $\boldsymbol{y}$ and $y{-}z = p$, it follows that $\boldsymbol{y} = \boldsymbol{q}\boldsymbol{z}$, where $\boldsymbol{q} = R_c(\boldsymbol{p})$, $c = (u{-}k) \bmod (v{-}u)$. Similarly, since $\boldsymbol{k}$ is a prefix of $\boldsymbol{z}$ and $z{-}k = p$, we see

that $\boldsymbol{z} = \boldsymbol{kp}$, hence that $\boldsymbol{y} = \boldsymbol{qkp}$. Thus $\boldsymbol{x} = (\boldsymbol{kp}^e)^2\boldsymbol{qkp}$, as claimed, and $\boldsymbol{x}$ and $\boldsymbol{kv}$ both have border $\boldsymbol{kp}$.

To see that $e > 1$, note that $k < \frac{v}{2}$, so that $e > \frac{v-u/2}{v-u} > 1$.

(f) Let $\boldsymbol{z} = \boldsymbol{v}[1..2u-(k+v)]$, nonempty prefix of $\boldsymbol{v}$ and suffix of $\boldsymbol{u}$.



Observe that

$$\boldsymbol{u}[k+j] = \boldsymbol{v}[j] = \boldsymbol{u}[(u-z)+j],\ 1 \leqslant j \leqslant z.$$

Thus $\boldsymbol{u}[k+1..u]$ has period $p = (u-z)-k = v-u$. Consider

$$\boldsymbol{y} = \boldsymbol{v}[u-k+1..v] = \boldsymbol{u}[1..(k+v)-u] = \boldsymbol{u}[1..k+p],$$

nonempty suffix of $\boldsymbol{v}$ and prefix of $\boldsymbol{u}$. Since $\boldsymbol{y}$ has prefix $\boldsymbol{k}$, it follows that $\boldsymbol{y} = \boldsymbol{kp}$, where $\boldsymbol{p} = \boldsymbol{u}[k+1..k+p]$. Thus for $e = \frac{u-k}{v-u}$, $\boldsymbol{v} = \boldsymbol{p}^e\boldsymbol{kp}$, $\boldsymbol{x} = \boldsymbol{k}(\boldsymbol{p}^e\boldsymbol{kp})^2$, as stated. Since $k+v < 2u$, $u-k > v-u$, and so $e > 1$.

(g) Let $\boldsymbol{z} = \boldsymbol{v}[2u-k+1..k+v]$, suffix of $\boldsymbol{v}$.

Observe that

$$\boldsymbol{v}[j] = \boldsymbol{u}[k+j] = \boldsymbol{v}[u+k+j],\ 1 \leqslant j \leqslant u-k,$$

so that $\boldsymbol{v}[1..2u-k]$ has period $p = u$. Then for $\boldsymbol{p} = \boldsymbol{u}[k+1..u]\boldsymbol{u}[1..k]$ and $e = \frac{2u-k}{u} \geqslant 1$, $\boldsymbol{v} = \boldsymbol{p}^e\boldsymbol{z}$ and $\boldsymbol{x} = \boldsymbol{k}(\boldsymbol{p}^e\boldsymbol{z})^2$. □

Case (g) of Lemma 8 is not a true overlap, but is included for completeness. Note also that cases (b), (c) and (f) require $k > 0$, and so do not exist if it is assumed that $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$ (or $\boldsymbol{v}^2$ and $\boldsymbol{w}^2$) occur at the same position. Overall, it turns out that analysis of overlapping squares requires breaking down the interval $[k, 2v)$ for u into seven highly nonuniform subintervals:

$$\left[k, \frac{k+v}{2}\right], \left(\frac{k+v}{2}, \frac{2(k+v)}{3}\right), \left[\frac{2(k+v)}{3}, v\right), \left[v\right], \left(v, \frac{k}{2}+v\right), \left[\frac{k}{2}+v, k+v\right], \left(k+v, 2v\right).$$

We make the observation that if a third square $\boldsymbol{w}^2$ begins to the right of the starting position of $\boldsymbol{v}^2$, sufficiently near to satisfy the postulates of Lemma 8,

then the analysis of the three squares $\boldsymbol{u}^2, \boldsymbol{v}^2, \boldsymbol{w}^2$ reduces to a simultaneous consideration of two of the lemma's cases. Thus, for example, the analysis of the situation shown in Figure 20 of Section 5 would take place in terms of the simultaneous occurrence of cases (e) (for $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$) and (b) (for $\boldsymbol{v}^2$ and $\boldsymbol{w}^2$). Indeed, all cases of three overlapping squares can be represented by pairs $[ij]$, $a \leqslant i, j \leqslant f$, referring to the cases (a)-(g) arising in Lemma 8.

4 Subcases 3 & 7 of the NPL

In this section we prove the two remaining subcases of Lemma 3.

4.1 Subcase 3

We first deal with the general case valid for all occurrences of Subcase 3, then go on to identify circumstances in which $\boldsymbol{x}$ is constrained to be a repetition of small period $d = \gcd(u, v, w)$.

Lemma 9 (Subcase 3). *Suppose that a string $\boldsymbol{x}$ has prefixes $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$, $3u/2 < v < 2u$, and suppose further that a third square $\boldsymbol{w}^2$, $w \neq u$, occurs at position $k+1$ of $\boldsymbol{x}$, where*

$$0 \leqslant k \leqslant u_1 < u_1 + u_2 < w < v \tag{6}$$

$$k + w \leqslant u \tag{7}$$

$$k + 2w > u + u_1 \tag{8}$$

and $u_1 = 2u - v$ and $u_2 = 2v - 3u$. Then $\boldsymbol{x} = \boldsymbol{d_1}^{u/d_1} \boldsymbol{d_1}^{v/d_1} \boldsymbol{d_1}^{(v-u)/d_1}$, where $d_1 = \gcd(u - w, v - u)$.

Proof. As we have seen (4), the overlap of $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$ forces $\boldsymbol{x} = (\boldsymbol{u_1 u_2 u_1 u_1 u_2})^2$, with $\boldsymbol{u} = \boldsymbol{u_1 u_2 u_1}$. By Lemma 8(a), $\boldsymbol{u} = \boldsymbol{p}^e \boldsymbol{z}$, where $\boldsymbol{z} = \boldsymbol{w}[1\,..\,u - (k + w)]$, $\boldsymbol{p} = \boldsymbol{u}[1\,..\,u - w]$ and $e = \frac{k+w}{u-w} > 1$.

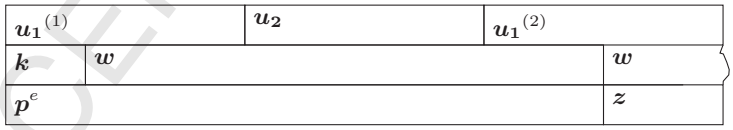


Fig. 3. String $\boldsymbol{u}$ in Subcase 3

We first show that if $\boldsymbol{u}$ has period $p = u - w$, the lemma holds. Note that $\boldsymbol{u}$ has period $u_1 + u_2$ and

$$u_1 + u_2 + p = u + u_1 + u_2 - w < u$$

since $u_1 + u_2 < w$ from (6). Therefore, assuming $\boldsymbol{u}$ has period p, $\boldsymbol{u} = \boldsymbol{x}[1\,..\,u]$ has period $d_1 = \gcd(p, u_1 + u_2)$ by Lemma 4. It follows that $\boldsymbol{u_1 u_2} = \boldsymbol{x}[u + v + 1\,..\,x]$,

a prefix of $\boldsymbol{u} = \boldsymbol{u_1 u_2 u_1}$, has period d_1 as well. Finally, $\boldsymbol{x}[u+1\,..\,u+v] = \boldsymbol{u_1 u_2 u_1 u_2 u_1}$ has period u_1+u_2 and prefix $\boldsymbol{u}$ of length $u > u_1+u_2$ with period d_1. Since $d_1 = \gcd(u-w, u_1+u_2)$ divides u_1+u_2, $\boldsymbol{x}[u+1\,..\,u+v]$ has period d_1 by Lemma 6. Thus the lemma holds assuming $\boldsymbol{u}$ has period p.

Note first from (6) and (7) that $u_1+u_2 < w < u$, hence that $u_1 - p = u_1-(u-w) > 0$. Then to see that $\boldsymbol{u}$ in fact has period p, consider two cases:

$$u_1 \geqslant k + w - (u_1+u_2) \geqslant p \tag{9}$$

and

$$k + w - (u_1+u_2) < p < u_1. \tag{10}$$

In the first case, the prefix $\boldsymbol{kw} = \boldsymbol{p}^e$ of $\boldsymbol{u}$ extends at least p positions into the suffix ${\boldsymbol{u_1}}^{(2)}$. Since $\boldsymbol{u_1}$ is a prefix of $\boldsymbol{kw}$, $\boldsymbol{u_1}$ has period p, and therefore $\boldsymbol{u}$ has a prefix and suffix of period p which overlap by at least p. Consequently, by Lemma 5, $\boldsymbol{u}$ has period p.

The second case (10) is more complicated (see Figure 4). Both $\boldsymbol{p}$ and $\boldsymbol{u_1}$ are prefixes of $\boldsymbol{u}$, so $\boldsymbol{p}$ is a proper prefix of $\boldsymbol{u_1}$. Both $\boldsymbol{u_1}$ and $\boldsymbol{z}$ are suffixes of $\boldsymbol{u}$, and

$$z = u - k - w \leqslant p < u_1,$$

so $\boldsymbol{z}$ is a proper suffix of $\boldsymbol{u_1}$. The prefix $\boldsymbol{p}$ and the suffix $\boldsymbol{z}$ of $\boldsymbol{u_1}$ must overlap because (10) is equivalent to $u_1 < p+z$. Noting that $p = u-w = k+z$ so that $\boldsymbol{p} = \boldsymbol{kz}$, we have (Figure 4)

$$\boldsymbol{z} = \boldsymbol{\ell' t'} = \boldsymbol{t'\ell} \tag{11}$$

and

$$\boldsymbol{u_1} = \boldsymbol{p\ell} = \boldsymbol{kz\ell} = \boldsymbol{k\ell' z} = \boldsymbol{k\ell' t'\ell}, \tag{12}$$

where $\boldsymbol{\ell}$ and $\boldsymbol{\ell'}$ are respectively the proper suffix and proper prefix of $\boldsymbol{z}$ of length $\ell = \ell' = u_1 - p$, and $\boldsymbol{t'}$ is the border of $\boldsymbol{z}$ of length $t' = z - \ell$. Since by (11) $\boldsymbol{z}$ has border $\boldsymbol{t'}$, it therefore has period ℓ, as does $\boldsymbol{\ell' z\ell} = \boldsymbol{\ell'\ell' t'\ell} = \boldsymbol{\ell' t'\ell\ell}$. Since $\boldsymbol{u_1}$ has period p, $\boldsymbol{p}$ has prefix $\boldsymbol{\ell}$; $\boldsymbol{p} = \boldsymbol{kz}$ also has suffix $\boldsymbol{\ell}$, so that $\boldsymbol{p}$ has border $\boldsymbol{\ell}$. Observe also that because $k+w-(u_1+u_2) = k+\ell$, $\boldsymbol{k\ell'}$ is the prefix of $\boldsymbol{u_1}$ that overlaps $\boldsymbol{w}$.

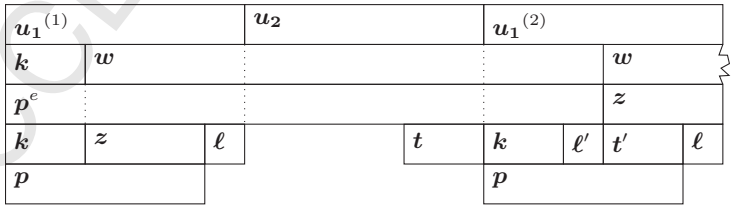


Fig. 4. String $\boldsymbol{u}$ in Subcase 3 when (10) holds

Let $\boldsymbol{t}$ be the suffix of $\boldsymbol{u_1 u_2}$ of length $t = t'$. Then $\boldsymbol{w}$ has suffix $\boldsymbol{tk\ell'}$ in which $\boldsymbol{k\ell'}$ is a prefix of $\boldsymbol{u_1}$. Recall $\boldsymbol{u_1} = \boldsymbol{k\ell' t'\ell}$ has period $p = k+t+\ell$. If $\boldsymbol{t} = \boldsymbol{t'}$, then

$\boldsymbol{tu_1}$ has period p; moreover, $\boldsymbol{kw} = \boldsymbol{p}^e$ and $\boldsymbol{tu_1}$ share substring $\boldsymbol{tk\ell'}$ of length p, so $\boldsymbol{u}$ has period p, as desired. Hence, it will suffice to show $\boldsymbol{t} = \boldsymbol{t'}$.

From $\boldsymbol{kw} = \boldsymbol{p}^e$, where $e > 1$, a complete copy of $\boldsymbol{p}$ occurs $h = \lfloor e \rfloor$ times in $\boldsymbol{kw}$. Three cases arise based on where in $\boldsymbol{u}$ the h^{th} occurrence of $\boldsymbol{p}$ ends:

(C1) $\boldsymbol{p}^{(h)}$ ends inside the suffix $\boldsymbol{t}$ of $\boldsymbol{u_2}$.
(C2) $\boldsymbol{p}^{(h)}$ ends inside the prefix $\boldsymbol{k}$ of $\boldsymbol{u_1}^{(2)}$.
(C3) $\boldsymbol{p}^{(h)}$ ends inside the suffix $\boldsymbol{\ell'}$ of $\boldsymbol{w}$.

We will see that $\boldsymbol{t} = \boldsymbol{t'}$ in each of these cases.

(C1)

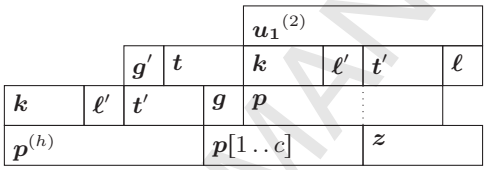


Fig. 5. Subcase 3 when (C1) holds

Suppose (C1) holds; that is, $\boldsymbol{p}^{(h)}$ ends inside the suffix $\boldsymbol{t}$ of $\boldsymbol{u_2}$. We introduce the ***gap*** $g = u_1 + u_2 - ph$, a measure of the overlap between $\boldsymbol{t}$ and the suffix $\boldsymbol{t'}$ of $\boldsymbol{p}^{(h)}$. Note that if $g = 0$, then $\boldsymbol{t} = \boldsymbol{t'}$ immediately. Let $\boldsymbol{g} = \boldsymbol{t}[t - g + 1 \,..\, t] = \boldsymbol{p}[1 \,..\, g]$ be the suffix of $\boldsymbol{t}$ that follows $\boldsymbol{p}^{(h)}$, and let $\boldsymbol{g'} = \boldsymbol{t'}[1 \,..\, g]$ be the prefix of $\boldsymbol{t'}$ that precedes $\boldsymbol{t}$. Also, let

$$c = (k + w) \bmod p = g + k + \ell$$

and observe that $\boldsymbol{kw}$ has suffix $\boldsymbol{p}[1 \,..\, c] = \boldsymbol{gk\ell'} = \boldsymbol{k\ell' g'}$.

Thus $\boldsymbol{p}[1 \,..\, c]$ has border $\boldsymbol{k\ell'}$ and therefore period g. String $\boldsymbol{\ell' g'}$ has period ℓ as a prefix of $\boldsymbol{z} = \boldsymbol{\ell' t'}$, and period g as a suffix of $\boldsymbol{p}[1 \,..\, c]$, so by Lemma 4 it has period $\gcd(g, \ell)$. Then $\boldsymbol{p}[1 \,..\, c]$ has period g and suffix $\boldsymbol{\ell' g'}$ of period $\gcd(g, \ell) \mid g$ and length $\ell + g \geqslant g$, so that by Lemma 6 $\boldsymbol{p}[1 \,..\, c]$ itself has period $\gcd(g, \ell)$. Both $\boldsymbol{p}[1 \,..\, c]$ and $\boldsymbol{\ell' z}$ have period ℓ and share substring $\boldsymbol{\ell'}$, so $\boldsymbol{p}[1 \,..\, c]\boldsymbol{z}$ has period ℓ by Lemma 5. It also has substring $\boldsymbol{p}$, so $\boldsymbol{p}$ has period ℓ. Because $\boldsymbol{p}$ has border $\boldsymbol{\ell}$ as well as period ℓ, any power of $\boldsymbol{p}$ has period ℓ. It follows that $\boldsymbol{kw} = \boldsymbol{p}^e$ has period ℓ and, since $\boldsymbol{p}[1 \,..\, c]\boldsymbol{z}$ has period ℓ and shares with $\boldsymbol{kw}$ a substring of length $c > \ell$, $\boldsymbol{u}$ has period ℓ by Lemma 5. Recall that $\boldsymbol{u}$ has substring $\boldsymbol{p}[1 \,..\, c]$ of period $\gcd(g, \ell) \mid \ell$, so $\boldsymbol{u}$ itself has period $\gcd(g, \ell)$ by Lemma 6. Recalling that $\boldsymbol{t}$ is a suffix of $\boldsymbol{t'g}$ and that both are substrings of $\boldsymbol{u}$, we find that $\boldsymbol{t}$ and $\boldsymbol{t'}$ have period $\gcd(g, \ell)$ and suffix $\boldsymbol{g}$, so $\boldsymbol{t} = \boldsymbol{t'}$.

(C2)

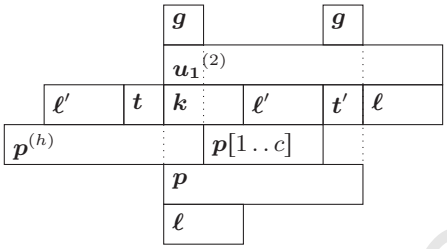


Fig. 6. Subcase 3 when (C2) holds

Suppose (C2) holds; that is, $\boldsymbol{p}^{(h)}$ ends inside the prefix $\boldsymbol{k}$ of $\boldsymbol{u_1}^{(2)}$. Let

$$g = ph - u_1 - u_2$$

be the overlap of $\boldsymbol{p}^{(h)}$ with $\boldsymbol{k}$, and let $\boldsymbol{g} = k[1\,..\,g]$. Note that if $g = 0$, then $\boldsymbol{t} = \boldsymbol{t}'$ immediately. Otherwise, $\boldsymbol{g}$ is a border of $\boldsymbol{p}$. Let

$$c = (k + w) \bmod p = k + \ell - g$$

and observe that, from the overlap of the suffix $\boldsymbol{p}[1\,..\,c]$ of $\boldsymbol{kw}$ and the prefix $\boldsymbol{p}$ of $\boldsymbol{u_1}$, $\boldsymbol{p}[1\,..\,k+\ell] = \boldsymbol{k\ell'}$ has period g. Also note that since by (12) $\boldsymbol{p} = \boldsymbol{k\ell' t'}$ and since $\boldsymbol{kw} = \boldsymbol{p}^e$ has period p, therefore $\boldsymbol{p}^{(h)}$ has suffix $\boldsymbol{\ell' tg}$. Consider four cases: $0 < g < \ell$, $g = \ell$, $\ell < g \leqslant z$, and $z < g$.

If $0 < g < \ell$, then since $\boldsymbol{\ell}$ is a prefix of $\boldsymbol{u_1}$, $\boldsymbol{\ell}$ has period g as a prefix of $\boldsymbol{k\ell'}$. Recall that $\boldsymbol{\ell}$ is also a suffix of $\boldsymbol{p}$, so $\boldsymbol{\ell}$ has border $\boldsymbol{g}$ and period $\ell - g$. Hence, by Lemma 4, $\boldsymbol{\ell}$ has period $\gcd(g, \ell - g) = \gcd(g, \ell)$. Recall also that $\boldsymbol{\ell' z}$ has period ℓ and substring $\boldsymbol{\ell}$ of period $\gcd(g, \ell) \mid \ell$, so by Lemma 6, $\boldsymbol{\ell' z}$ has period $\gcd(g, \ell)$. Prefix $\boldsymbol{\ell'}$ of $\boldsymbol{\ell' z}$ then has period $\gcd(g, \ell) \mid g$, and since $\boldsymbol{\ell'}$ is also a suffix of the string $\boldsymbol{k\ell'}$ of period g, $\boldsymbol{k\ell'}$ has period $\gcd(g, \ell)$ by Lemma 6. Since $\boldsymbol{\ell' z}$ and $\boldsymbol{k\ell'}$ have period $\gcd(g, \ell)$, $\boldsymbol{u_1} = \boldsymbol{k\ell' z}$ has period $\gcd(g, \ell)$ by Lemma 5. Both $\boldsymbol{tg}$ and $\boldsymbol{t'g}$ are substrings of $\boldsymbol{u_1}$, so $\boldsymbol{t} = \boldsymbol{t}'$.

If $g = \ell$, then $\boldsymbol{p}$ has suffixes $\boldsymbol{t\ell}$ and $\boldsymbol{z} = \boldsymbol{\ell' t} = \boldsymbol{t'\ell}$, so immediately $\boldsymbol{t} = \boldsymbol{t}'$. Note that $\boldsymbol{k\ell'}$ and $\boldsymbol{\ell' z}$ have period $g = \ell$, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{k\ell' t'}$ has period ℓ.

If $\ell < g \leqslant z$, then since $\boldsymbol{\ell}$ is a border of $\boldsymbol{g}$, $\boldsymbol{g}$ has period $g - \ell$; it also has period ℓ as a substring of the suffix $\boldsymbol{z}$ of $\boldsymbol{p}$, and thus by Lemma 4 period $\gcd(g, g - \ell) = \gcd(g, \ell)$. String $\boldsymbol{g}$ is a substring of $\boldsymbol{k\ell'}$, which as we have seen has period g, so that by Lemma 6, $\boldsymbol{k\ell'}$ has period $\gcd(g, \ell)$. Since $\boldsymbol{\ell' z}$ and $\boldsymbol{k\ell'}$ have period $\gcd(g, \ell)$, $\boldsymbol{u_1} = \boldsymbol{k\ell' z}$ has period $\gcd(g, \ell)$ by Lemma 5. Both $\boldsymbol{tg}$ and $\boldsymbol{t'g}$ are substrings of $\boldsymbol{u_1}$, so $\boldsymbol{t} = \boldsymbol{t}'$.

If $z < g$, then, as shown in Figure 7, the suffix $\boldsymbol{z}$ of $\boldsymbol{p}^{(h)}$ is a substring of the prefix $\boldsymbol{k}$ of $\boldsymbol{u_1}$, and $\boldsymbol{\ell' t}$ is a substring of the prefix $\boldsymbol{k}$ of $\boldsymbol{p}^{(h)}$. $\boldsymbol{k}$ also has two

borders $\boldsymbol{g_1}$ and $\boldsymbol{g_2}$: $\boldsymbol{g_1}$ is the border of $\boldsymbol{k}$ of length $g_1 = k - g$ resulting from the overlap of the prefix $\boldsymbol{k}$ of $\boldsymbol{u_1}$ with $\boldsymbol{p}[1\,..\,c] = \boldsymbol{k}[1\,..\,c]$, while $\boldsymbol{g_2}$ is the border of $\boldsymbol{k}$ of length $g_2 = g - z$ resulting from the overlap of the prefix $\boldsymbol{k}$ of $\boldsymbol{p}^{(h)}$ with the prefix $\boldsymbol{k}$ of $\boldsymbol{u_1}$. We then have $\boldsymbol{k} = \boldsymbol{g_1\ell' t g_2} = \boldsymbol{g_2\ell' t' g_1}$. Also recall that $\boldsymbol{\ell}$ is a prefix of $\boldsymbol{p} = \boldsymbol{kz}$, so that either $\boldsymbol{\ell}$ is a prefix of $\boldsymbol{g_1}$ or $\boldsymbol{g_1}$ is a prefix of $\boldsymbol{\ell}$.

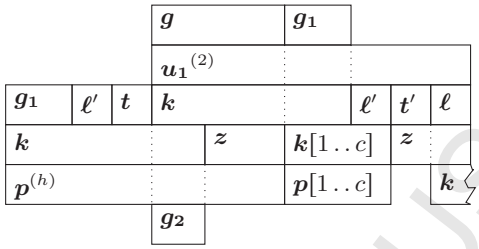


Fig. 7. Subcase 3 when (C2) holds and $z < g$

If $g_1 = g_2$, then $\boldsymbol{t} = \boldsymbol{t'}$ immediately. If $g_1 \neq g_2$, then several cases arise:

1. $g_1 < g_2$

   Let $g' = g'' = g_2 - g_1$, let $\boldsymbol{g'}$ be the prefix of $\boldsymbol{g_2}$ such that $\boldsymbol{g_2} = \boldsymbol{g'g_1}$, and let $\boldsymbol{g''}$ be the suffix of $\boldsymbol{g_2}$ such that $\boldsymbol{g_2} = \boldsymbol{g_1 g''}$. Observe that $\boldsymbol{g_1}$ is a border of $\boldsymbol{g_2}$, so $\boldsymbol{g_2}$ has period g'.

   (a) $g' \leqslant z$

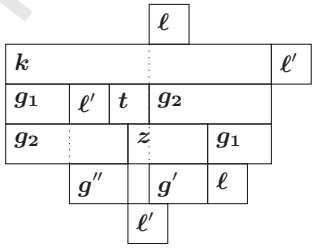


Fig. 8. Subcase 3 when (C2) holds, $z < g$, and $g_1 < g_2$

The demonstration requires several steps:

- $\boldsymbol{g'\ell}$ has period ℓ as a suffix of $\boldsymbol{z\ell}$; it also has border $\boldsymbol{\ell}$ and period g', so by Lemma 4, $\boldsymbol{g'\ell}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{z\ell}$ has period ℓ and suffix $\boldsymbol{g'\ell}$ of period $\gcd(g', \ell) \mid \ell$, so by Lemma 6, $\boldsymbol{z\ell}$ has period $\gcd(g', \ell)$.

- $\boldsymbol{g_2}$ has period g' and prefix $\boldsymbol{g'}$ of period $\gcd(g', \ell) \mid g'$, so by Lemma 6, $\boldsymbol{g_2}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{z\ell}$ and $\boldsymbol{g_2}$ have period $\gcd(g', \ell)$ and share substring $\boldsymbol{g'}$, so by Lemma 5, $\boldsymbol{zg_1}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{g''\ell'}$ has border $\boldsymbol{\ell'}$ and period $g' = g''$; it also has prefix $\boldsymbol{g''}$ which, as a suffix of $\boldsymbol{g_2}$, has period $\gcd(g', \ell) \mid g'$, so by Lemma 6, $\boldsymbol{g''\ell'}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{g_2}$ and $\boldsymbol{g''\ell'}$ have period $\gcd(g', \ell)$ and share substring $\boldsymbol{g''}$, so by Lemma 5, $\boldsymbol{g_2\ell'}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{g_2\ell'}$ and $\boldsymbol{zg_1}$ have period $\gcd(g', \ell)$ and share substring $\boldsymbol{\ell'}$, so by Lemma 5, $\boldsymbol{k} = \boldsymbol{g_2zg_1}$ has period $\gcd(g', \ell)$.

Since $\boldsymbol{\ell' t}$ and $\boldsymbol{\ell' t'}$ are substrings of $\boldsymbol{k}$, therefore $\boldsymbol{t} = \boldsymbol{t'}$.
Note that $\boldsymbol{g''z\ell}$ has period $\gcd(g', \ell)$, so that $\boldsymbol{k} = \boldsymbol{g_1\ell' tg_1 g''}$ and $\boldsymbol{g''z\ell}$ have period $\gcd(g', \ell)$ and share substring $\boldsymbol{g''}$, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{kz\ell}$ has period $\gcd(g', \ell)$.

(b) $g' > z$

$\boldsymbol{k}$ has period $k - g_2 = g_1 + z$, so $\boldsymbol{k}$ has a prefix $\boldsymbol{g_1\ell' tg'_2} = \boldsymbol{g'_2zg_1}$, where $\boldsymbol{g'_2}$ is a prefix of $\boldsymbol{g_2}$ and $|g'_2 - g_1| \leqslant z$, so one of cases 1(a) and 2(a) applies.

2. $g_1 > g_2$

Let $g' = g_1 - g_2$, and let $\boldsymbol{g'}$ be the suffix of $\boldsymbol{g_1}$ such that $\boldsymbol{g_1} = \boldsymbol{g_2g'}$. Observe that $\boldsymbol{g_2}$ is a border of $\boldsymbol{g_1}$, so $\boldsymbol{g_1}$ and $\boldsymbol{g_2}$ have period g'.

(a) $g' \leqslant z$ (Figures 9 & 10)

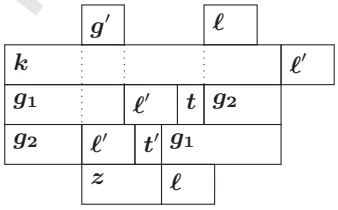


Fig. 9. Subcase 3 when (C2) holds, $z < g$, $g_1 > g_2$, and $g' \leqslant \ell$

Again several steps are required:

- $\boldsymbol{g'\ell'}$ has period ℓ as a prefix of $\boldsymbol{z\ell}$ and also shares prefix $\boldsymbol{\ell'}$ with $\boldsymbol{z}$, so it has border $\boldsymbol{\ell'}$ and period g'.
- $\boldsymbol{g'\ell'}$ has periods ℓ and g', so by Lemma 4, $\boldsymbol{g'\ell'}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{g_1}$ has period g' and suffix $\boldsymbol{g'}$ of period $\gcd(g', \ell) \mid g'$, so by Lemma 6, $\boldsymbol{g_1}$ has period $\gcd(g', \ell)$.

- $\boldsymbol{z\ell}$ has period ℓ and prefix $\boldsymbol{g'}$ of period $\gcd(g', \ell) \mid \ell$, so again by Lemma 6, $\boldsymbol{z\ell}$ has period $\gcd(g', \ell)$.
- $\boldsymbol{z\ell}$ and $\boldsymbol{g_1}$ have period $\gcd(g', \ell)$ and share a substring of length at least $\min(g', \ell)$, so by Lemma 5, $\boldsymbol{zg_1}$ has period $\gcd(g', \ell)$.

Since $\boldsymbol{\ell' t}$ and $\boldsymbol{\ell' t'}$ are substrings of $\boldsymbol{zg_1}$, therefore $\boldsymbol{t} = \boldsymbol{t'}$.
Note that $\boldsymbol{g_1}$ and $\boldsymbol{zg_1}$ have period $\gcd(g', \ell)$ and share substring $\boldsymbol{g'}$, so by Lemma 5, $\boldsymbol{k} = \boldsymbol{g_2 z g_1}$ has period $\gcd(g', \ell)$. $\boldsymbol{g' z\ell}$ then has period $\gcd(g', \ell)$, so that $\boldsymbol{k} = \boldsymbol{g_2 z g_2 g'}$ and $\boldsymbol{g' z\ell}$ have period $\gcd(g', \ell)$ and share substring $\boldsymbol{g'}$, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{kz\ell}$ has period $\gcd(g', \ell)$.

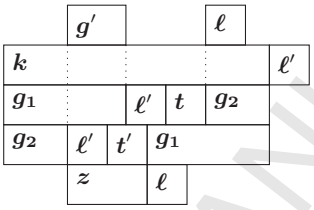


Fig. 10. Subcase 3 when (C2) holds, $z < g$, $g_1 > g_2$, and $\ell < g' \leqslant z$

(b) $g' > z$

$\boldsymbol{k}$ has period $k - g_1 = g_2 + z$, so $\boldsymbol{k}$ has a prefix $\boldsymbol{g_2 z g'_1} = \boldsymbol{g'_1 \ell' t g_2}$, where $\boldsymbol{g'_1}$ is a prefix of $\boldsymbol{g_1}$ and $|g'_1 - g_2| \leqslant z$, so one of cases 1(a) and 2(a) applies.

(C3)

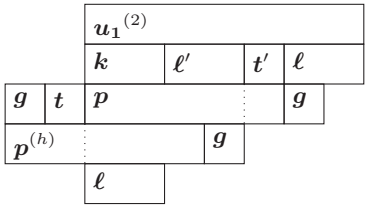


Fig. 11. Subcase 3 when (C3) holds

Suppose (C3) holds; that is, $\boldsymbol{p}^{(h)}$ ends inside the suffix $\boldsymbol{\ell'}$ of $\boldsymbol{w}$. Let $g = k + w - ph$ and let $\boldsymbol{g} = \boldsymbol{\ell'}[\ell - g + 1 \,..\, \ell]$ be the suffix of $\boldsymbol{\ell'}$ that follows $\boldsymbol{p}^{(h)}$. Because $\boldsymbol{kw}$ (of which $\boldsymbol{\ell'}$ is a suffix) has period p, $\boldsymbol{g}$ is a prefix of $\boldsymbol{p}$. Recall that $\boldsymbol{\ell}$ is a prefix of

$\boldsymbol{p}$, so $\boldsymbol{g}$ is also a prefix of $\boldsymbol{\ell}$. From $\boldsymbol{p}^{(h)}$ and the occurrence of $\boldsymbol{p}$ that prefixes $\boldsymbol{u_1}$, we have

$$\boldsymbol{p} = \boldsymbol{gtk}(\boldsymbol{\ell}'[1\,..\,\ell - g]) = \boldsymbol{k}(\boldsymbol{\ell}'[1\,..\,\ell - g])\boldsymbol{gt}'$$

and $\boldsymbol{p}$ has period $t+g$.

Consider the string $\boldsymbol{\ell}'\boldsymbol{t}'\boldsymbol{g}$, which occurs near the end of $\boldsymbol{u_1}$ as a prefix of $\boldsymbol{\ell}'\boldsymbol{t}'\boldsymbol{\ell} = \boldsymbol{\ell}'\boldsymbol{z}$. As a substring of $\boldsymbol{\ell}'\boldsymbol{z} = \boldsymbol{\ell}'\boldsymbol{\ell}'\boldsymbol{t}'$, it has period ℓ. Since $\boldsymbol{p}$ has period $t+g$ and suffixes $\boldsymbol{\ell}'\boldsymbol{t}'$ and $\boldsymbol{gt}'$, $\boldsymbol{\ell}'\boldsymbol{t}'\boldsymbol{g}$ also has period $t+g$. $\boldsymbol{\ell}'\boldsymbol{t}'\boldsymbol{g}$ has periods $t+g$ and ℓ, so by Lemma 4, it has period $\gcd(t+g,\ell)$. Now $\boldsymbol{p}$ has period $t+g$ and suffix $\boldsymbol{gt}'$ of period $\gcd(t+g,\ell) \mid t+g$, so $\boldsymbol{p}$ itself has period $\gcd(t+g,\ell)$. Because $\boldsymbol{p}$ has border $\boldsymbol{\ell}$ as well as period $\gcd(t+g,\ell)$, any power of $\boldsymbol{p}$ has period $\gcd(t+g,\ell)$. Thus $\boldsymbol{kw} = \boldsymbol{p}^e$ has period $\gcd(t+g,\ell)$ and, since $\boldsymbol{\ell}'\boldsymbol{z}$ has period $\gcd(t+g,\ell)$ and shares with $\boldsymbol{kw}$ a substring of length ℓ, $\boldsymbol{u}$ has period $\gcd(t+g,\ell)$ by Lemma 5. Since $\boldsymbol{t\ell}$ and $\boldsymbol{t}'\boldsymbol{\ell}$ are substrings of $\boldsymbol{u}$, therefore $\boldsymbol{t} = \boldsymbol{t}'$.

This completes the proof of Subcase 3. □

Lemma 10. *Suppose the conditions of Subcase 3 hold (Lemma 9). Then* $\boldsymbol{x} = \boldsymbol{d}^{x/d}$*, except possibly for*

1. $k+2w \geqslant v$ **or**
2. $k+2w < v$ **and**
   (a) $v-u = h(u-w)$ **or**
   (b) $v-u = (h-\frac{1}{2})(u-w)$,

where $d = \gcd(u,v,w)$ *and* $h = \left\lfloor \frac{k+w}{u-w} \right\rfloor$.

Proof. Note first that conditions 1 and 2 are simply reformulations of inequalities (9) and (10), respectively, found at the beginning of the proof of Lemma 9, where $v-u$ and $u-w$ replace u_1+u_2 and p, respectively. These inequalities constitute the two main cases considered in the proof, and so the result holds for condition 1.

Condition 2 however breaks down into cases (C1)-(C3). For both (C1) and (C3), it is shown that $\boldsymbol{u_1}$ has period ℓ (all symbols used as defined in the proof of Lemma 9). The same is true also for the various subcases of (C2), except when

(a′) the gap $g = 0$ **or**
(b′) $z < g$ and $g_1 = g_2$.

In all other cases, it is shown that $\boldsymbol{u_1} = \boldsymbol{kz\ell} = \boldsymbol{p\ell}$ has period ℓ. Then, by Lemma 9, $\boldsymbol{u} = \boldsymbol{u_1u_2u_1}$ has period $d_1 = \gcd(p, u_1+u_2)$. Hence $\boldsymbol{p}$ is a suffix of $\boldsymbol{u_1}$, thus a border of $\boldsymbol{u}$. Therefore $\boldsymbol{u}^2$ has period d_1, as well as period u, so that by Lemma 4, $\boldsymbol{u}^2$ has period $\gcd(u,d_1) = \gcd(u,\gcd(u-w,v-u)) = \gcd(u,v,w) = d$. This periodicity clearly extends to all of $\boldsymbol{x}$.

Next observe that in the proof of Lemma 9, $g = u_1+u_2-ph$, so that the condition $g = 0$ given in (a′) converts to the condition of (a) using the indicated substitutions for u_1+u_2 and p. Again from the proof of Lemma 9, we find that when $z < g$, $g_1 = k-g$, $g_2 = g-z$, from which we conclude that $p = k+z = 2g$ in (b′). This in turn implies that h copies of $\boldsymbol{p}$ ($2h$ copies of $\boldsymbol{g}$) cover $\boldsymbol{u_1u_2g}$ of length $v-u+g$, from which (b) follows. □

4.2 Subcase 7

Here we give results for Subcase 7 corresponding to those for Subcase 3:

Lemma 11 (Subcase 7). *Suppose that a string $\boldsymbol{x}$ has prefixes $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$, $3u/2 < v < 2u$, and suppose further that a third square $\boldsymbol{w}^2$, $w \neq u$, occurs at position $k+1$ of $\boldsymbol{x}$, where*

$$u_1 < k < u_1 + u_2 < w < v \tag{13}$$

$$k + w \leqslant u + u_1 \tag{14}$$

$$k + 2w \leqslant 2u \tag{15}$$

and $u_1 = 2u - v$ and $u_2 = 2v - 3u$. Then $\boldsymbol{x} = \boldsymbol{d_1}^{u/d_1}\boldsymbol{d_1}^{v/d_1}\boldsymbol{d_1}^{(v-u)/d_1}$, where $d_1 = \gcd(u - w, v - u)$.

Proof. As we have seen (4), the overlap of $\boldsymbol{u}^2$ and $\boldsymbol{v}^2$ forces $\boldsymbol{x} = (\boldsymbol{u_1u_2u_1u_1u_2})^2$, with $\boldsymbol{u} = \boldsymbol{u_1u_2u_1}$. By Lemma 8(b), $\boldsymbol{u} = \boldsymbol{zp}^e$, where $\boldsymbol{z} = \boldsymbol{u}[1\,..\,k + w - u]$, $\boldsymbol{p} = \boldsymbol{w}[1\,..\,u - w]$, and $e = 1 + \frac{u-k}{u-w}$. See Figure 12.

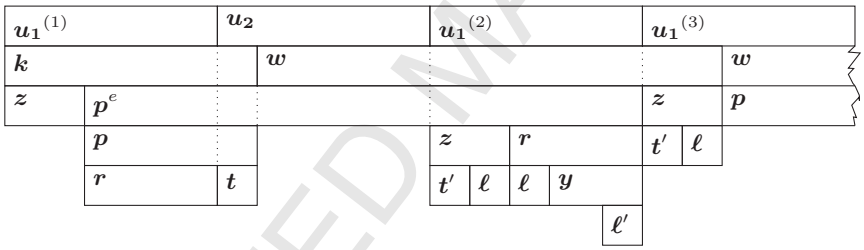


Fig. 12. String $\boldsymbol{uu_1}$ in Subcase 7

We first show that if $\boldsymbol{u}$ has period $p = u - w$, the lemma holds. Note that $\boldsymbol{u}$ has period $u_1 + u_2$ and

$$u_1 + u_2 + p = u + u_1 + u_2 - w < u$$

since $u_1 + u_2 < w$ from (13). Assuming $\boldsymbol{u}$ has period p, $\boldsymbol{u} = \boldsymbol{x}[1\,..\,u]$ has period $d_1 = \gcd(p, u_1+u_2)$ by Lemma 4. It follows that $\boldsymbol{u_1u_2} = \boldsymbol{x}[u+v+1\,..\,x]$, a prefix of $\boldsymbol{u} = \boldsymbol{u_1u_2u_1}$, has period d_1 as well. Finally, $\boldsymbol{x}[u + 1\,..\,u + v] = \boldsymbol{u_1u_2u_1u_2u_1}$ has period $u_1 + u_2$ and prefix $\boldsymbol{u}$ of length $u > u_1 + u_2$ with period d_1. Since $d_1 = \gcd(u-w, u_1+u_2)$ divides u_1+u_2, $\boldsymbol{x}[u+1\,..\,u+v]$ has period d_1 by Lemma 6. Thus the lemma holds assuming $\boldsymbol{u}$ has period p.

We now embark on a demonstration that $\boldsymbol{u}$ has period p. Notice (Figure 12) that $\boldsymbol{u_1u_2}$, $\boldsymbol{k}$, and $\boldsymbol{zp}$ are prefixes of $\boldsymbol{u}$. Given that $z = k-p$, that $k \in (u_1, u_1+u_2)$ by (13), and that $z \leqslant u_1$ by (14), we have

$$\boldsymbol{k} = \boldsymbol{zp} = \boldsymbol{zrt} = \boldsymbol{u_1t}, \tag{16}$$

where $\boldsymbol{r} = \boldsymbol{u_1}[z+1, u_1]$, and $\boldsymbol{t} = \boldsymbol{u_2}[1\,..\,k-u_1]$.

Observe that

$$z-p = (k+w-u) - (u-w) = k - (2u-2w) \leqslant 0$$

by (15), so that $p \geqslant z$. Also, by (13)

$$z = k+w-u > k+u_1+u_2-u = k-u_1 > 0,$$

so that in fact $z \geqslant 2$. Note further from (13) that

$$p = u-w < u - (u_1+u_2) = u_1,$$

while from (15) and (13),

$$p = u-w \geqslant k/2 > u_1/2. \tag{17}$$

Thus $u_1/2 < k/2 \leqslant p < u_1$. Putting these inequalities together, we find

$$2 \leqslant z \leqslant p < u_1 = z+r, \tag{18}$$

from which we conclude that $r > 0$.

Also, since

$$z \leqslant p = r+t < u_1 = r+z,$$

and recalling from (13) that $t = k-u_1 > 0$, we see that $0 < t < z$, where since $k = z+p \geqslant 2z$, $z \leqslant k/2$. Hence

$$0 < t < z \leqslant k/2 \leqslant p < u_1.$$

Let $\boldsymbol{t'}$ be the prefix of $\boldsymbol{z}$ of length t. Since $t' = t < z$ and $\boldsymbol{u_1 z}$ is a suffix of $\boldsymbol{w}^{(1)}$, there exists within $\boldsymbol{w}$ a complete occurrence of $\boldsymbol{u_1 t'}$.

Since $\boldsymbol{w}^{(1)}$ has prefix $\boldsymbol{p}$, so also does $\boldsymbol{w}^{(2)}$, with $\boldsymbol{p} = \boldsymbol{rt}$. Furthermore $\boldsymbol{k} = \boldsymbol{zrt} = \boldsymbol{zp}$, so that $\boldsymbol{p}$ is a suffix of $\boldsymbol{k}$ with nonempty prefix $\boldsymbol{r}$ that is a suffix of $\boldsymbol{u_1}$. Since $\boldsymbol{u_1}$ is a proper substring of $\boldsymbol{w}^{(1)}$ and $p < u_1$, it follows that $\boldsymbol{u_1}$ has period p. In fact, the string

$$\boldsymbol{u'} = R_z(\boldsymbol{u}) = \boldsymbol{p}^e\boldsymbol{z} = \boldsymbol{pw} = \boldsymbol{ru_2u_1z}$$

has period p. Then $\boldsymbol{u_1} = \boldsymbol{zr}$, $\boldsymbol{rz}$ and $\boldsymbol{u_1 z} = \boldsymbol{zrz}$ all have period p.

Again by the periodicity of $\boldsymbol{u'}$, there exists a possibly empty $\boldsymbol{y'}$ such that $\boldsymbol{p_1} = \boldsymbol{zy'}$ is a prefix of $\boldsymbol{u_1}$, and a $\boldsymbol{y}$, with $y = y' = p-z$, such that $\boldsymbol{p_2} = \boldsymbol{zy}$ is a suffix of $\boldsymbol{u_1}$, where $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$ are both rotations of $\boldsymbol{p}$.

Now consider $\boldsymbol{u_1 z}$, a suffix of $\boldsymbol{u'}$ with period p: this string has prefix $\boldsymbol{zy'z}$ and suffix $\boldsymbol{zyz}$ which overlap each other by

$$\hat{p} = u_1+z-2u_1+2p = p+(p+z)-u_1 > p$$

positions. We may therefore conclude that all substrings of length p in $\boldsymbol{zy'z}$ and $\boldsymbol{zyz}$ are rotations of each other. Then $\boldsymbol{u_1}$ and $R_z(\boldsymbol{u_1})$ both have period p, and so,

since $\ell = u_1{-}p = z{-}t < z$, we can apply Lemma 7(a) (with $(x, v, u) \sim (u_1, z, p)$) to conclude that $R_t(\boldsymbol{u_1})[1..2(z{-}t)]$ is a square of period ℓ. Thus we may write $\boldsymbol{u_1} = \boldsymbol{t'\ell}^2 \cdots$, where $\boldsymbol{t'\ell} = \boldsymbol{z}$. In fact, since $p = z{+}y = u_1{-}\ell$, so that $u_1 = z{+}\ell{+}y$, we find that $\boldsymbol{u_1} = \boldsymbol{t'\ell}^2\boldsymbol{y}$ with $\boldsymbol{z} = \boldsymbol{t'\ell}$, $\boldsymbol{r} = \boldsymbol{\ell y}$ and $\boldsymbol{p} = \boldsymbol{\ell y t}$.

Since $\boldsymbol{u'} = \boldsymbol{pw}$ has period p, $\boldsymbol{w}$ is a prefix of $\boldsymbol{u'}$. As we see from Figure 12, this prefix $\boldsymbol{w}$ ends distance $r{+}t = \ell{+}y{+}t' = y{+}t'{+}\ell$ before the end of $\boldsymbol{w}^{(1)}$, from which we conclude that $\boldsymbol{w}$ has suffix $\boldsymbol{t'\ell\ell}$ as well as suffix $\boldsymbol{z} = \boldsymbol{t'\ell}$. Thus $\boldsymbol{t'}$ is a border of $\boldsymbol{z}$. Now let $\boldsymbol{\ell'}$ be the prefix of $\boldsymbol{z}$ of length ℓ, so that $\boldsymbol{z} = \boldsymbol{t'\ell} = \boldsymbol{\ell' t'}$ has period ℓ. Note further that since $\boldsymbol{w}$ has suffix $\boldsymbol{yz}$, which in turn has suffix $\boldsymbol{t'\ell\ell} = \boldsymbol{\ell' t'\ell}$, therefore $\boldsymbol{\ell'}$ is a suffix of $\boldsymbol{y}$.

Assume $\boldsymbol{t} = \boldsymbol{t'}$. Then $\boldsymbol{k} = \boldsymbol{zrt} = \boldsymbol{zrt'}$ occurs in $\boldsymbol{w}$, and as $\boldsymbol{w}$ has period p, so does $\boldsymbol{k}$. $\boldsymbol{u}$ then has prefix $\boldsymbol{k} = \boldsymbol{zp}$ and suffix $\boldsymbol{p}^e$ both of period p and both including $\boldsymbol{p}$, so by Lemma 5, $\boldsymbol{u}$ has period p, as desired. Hence it will suffice to show $\boldsymbol{t} = \boldsymbol{t'}$.

From (18) it follows that a complete copy of $\boldsymbol{p}$ occurs $h \geqslant 2$ times in $\boldsymbol{u'}$. Several cases arise, based on the position of the suffix $\boldsymbol{t}$ of the h^{th} occurrence of $\boldsymbol{p}$:

(C1) $\boldsymbol{t}$ ends inside the prefix $\boldsymbol{z}$ of $\boldsymbol{u_1}^{(3)}$
(C2) $\boldsymbol{t}$ is a substring of the suffix $\boldsymbol{y}$ of $\boldsymbol{u_1}^{(2)}$, but $\boldsymbol{t\ell}$ is not.
(C3) $\boldsymbol{t\ell}$ is a substring of the suffix $\boldsymbol{y}$ of $\boldsymbol{u_1}^{(2)}$.
(C4) $\boldsymbol{t}$ begins to the left of the suffix $\boldsymbol{y}$ of $\boldsymbol{u_1}^{(2)}$ and ends inside $\boldsymbol{y}$.

We will see $\boldsymbol{t} = \boldsymbol{t'}$ in all of these cases.

(C1)

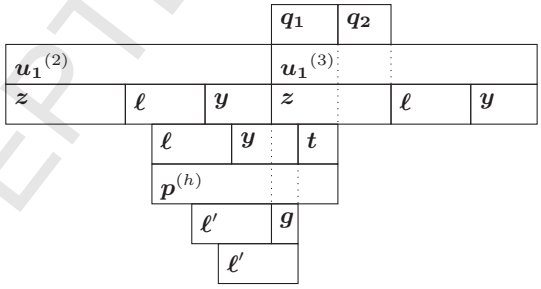


Fig. 13. Subcase 7 when (C1) holds and $g > 0$

Suppose first that (C1) holds, and write $\boldsymbol{z} = \boldsymbol{q_1 q_2}$, where $\boldsymbol{q_1}$ is a nonempty suffix of $\boldsymbol{p}$ and, by the periodicity of $\boldsymbol{u'}$, $\boldsymbol{q_2}$ is a prefix of $\boldsymbol{p}$.

We have shown that $\boldsymbol{u'} = \boldsymbol{p}^h\boldsymbol{q_2}$, where $\boldsymbol{p} = \boldsymbol{\ell y t}$, and so $\boldsymbol{u'} = \boldsymbol{p}^{h-1}(\boldsymbol{\ell y})(\boldsymbol{t})\boldsymbol{q_2}$. As in the proof of Lemma 9, we introduce the ***gap*** $g = q_1{-}t$, a measure of the overlap between the prefix $\boldsymbol{q_1}$ of $\boldsymbol{u_1}^{(3)}$ and the suffix $\boldsymbol{t}$ of $\boldsymbol{p}^{(h)}$. If $g \geqslant 0$, then $\boldsymbol{t}$

is a substring of $\boldsymbol{z}$; otherwise, $\boldsymbol{t}$ ends inside $\boldsymbol{z}$ but begins before it. Note that if $g = 0$, then $\boldsymbol{q_1} = \boldsymbol{t} = \boldsymbol{t'}$ and the remainder of the proof follows.

Suppose then that $g > 0$ (Figure 13), so that $\boldsymbol{q_1} = \boldsymbol{gt}$ for some string $\boldsymbol{g}$ of length g. In this case, note that $\boldsymbol{\ell' t}$ and $\boldsymbol{\ell' t'}$ are substrings of $\boldsymbol{\ell' z} = \boldsymbol{\ell' \ell' t'}$, as we have seen of period ℓ, and so both these strings also have period ℓ, implying that $\boldsymbol{t} = \boldsymbol{t'}$, as required.

We now show further that for $g > 0$, $\boldsymbol{u_1}$ has period $\gcd(g, \ell)$. Since $\boldsymbol{t}$ is a substring of $\boldsymbol{z} = \boldsymbol{t'\ell}$, $g \leqslant \ell$. Therefore, since $\boldsymbol{\ell y}$ is a suffix of $\boldsymbol{u_1}$ and $\boldsymbol{p} = \boldsymbol{\ell y t}$, $\boldsymbol{\ell y}$ and $\boldsymbol{\ell}$ both have period g, as does $\boldsymbol{\ell'}$, since it is a suffix of $\boldsymbol{\ell y}$. Observe that $\boldsymbol{\ell' g}$ has period ℓ as a prefix of $\boldsymbol{\ell' z}$, as well as period g as a suffix of $\boldsymbol{\ell y}$, so that by Lemma 4, $\boldsymbol{\ell' g}$ has period $\gcd(g, \ell)$. $\boldsymbol{z\ell}$ then has period ℓ and a substring $\boldsymbol{\ell'}$ of period $\gcd(g, \ell) \mid \ell$, so by Lemma 6, $\boldsymbol{z\ell}$ has period $\gcd(g, \ell)$. $\boldsymbol{\ell y}$ has period g and suffix $\boldsymbol{g}$ of period $\gcd(g, \ell)$, so by Lemma 6, it has period $\gcd(g, \ell)$. $\boldsymbol{z\ell}$ and $\boldsymbol{\ell y}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{\ell}$, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{z\ell y}$ has period $\gcd(g, \ell)$.

Suppose next that $g < 0$, so that $\boldsymbol{t} = \boldsymbol{gq_1}$ for some string $\boldsymbol{g}$ of length $|g|$, as shown in Figure 14. Again $\boldsymbol{\ell y}$ and $\boldsymbol{\ell}$ both have period $|g|$. If $|g| \leqslant \ell$, then $\boldsymbol{t\ell}$ is a substring of $\boldsymbol{\ell' z}$, so $\boldsymbol{t} = \boldsymbol{t'}$. However, when $g < 0$, it is possible that $|g| > \ell$. In general, let $\boldsymbol{g'}$ be the suffix of $\boldsymbol{z}$ of length $|g|$. The suffix $\boldsymbol{q_2} = \boldsymbol{\ell g'}$ of $\boldsymbol{z}$ has border $\boldsymbol{\ell}$ and thus period $q_2 - \ell = |g|$. It also has period ℓ as a suffix of $\boldsymbol{z}$, so by Lemma 4, it has period $\gcd(g, \ell)$. $\boldsymbol{\ell' z}$ then has period ℓ and suffix $\boldsymbol{\ell g'}$ of period $\gcd(g, \ell) \mid \ell$, so that by Lemma 6, $\boldsymbol{\ell' z}$ has period $\gcd(g, \ell)$. Also by Lemma 6, $\boldsymbol{\ell y}$ has period $\gcd(g, \ell)$ since it has period $|g|$ and, by the periodicity of $\boldsymbol{u'}$, substring $\boldsymbol{g'}$ of period $\gcd(g, \ell) \mid |g|$. Both $\boldsymbol{\ell y}$ and $\boldsymbol{\ell' z}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{\ell'}$, so that by Lemma 5, $\boldsymbol{\ell yz}$ has period $\gcd(g, \ell)$. Since $\boldsymbol{t\ell}$ and $\boldsymbol{t'\ell}$ are both substrings of $\boldsymbol{\ell yz}$, therefore again $\boldsymbol{t} = \boldsymbol{t'}$.

Note finally that since $\boldsymbol{z\ell}$ and $\boldsymbol{\ell y}$ both have period $\gcd(g, \ell)$ and share substring $\boldsymbol{\ell}$, therefore by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{z\ell y}$ again has period $\gcd(g, \ell)$, as it did also for $g > 0$.

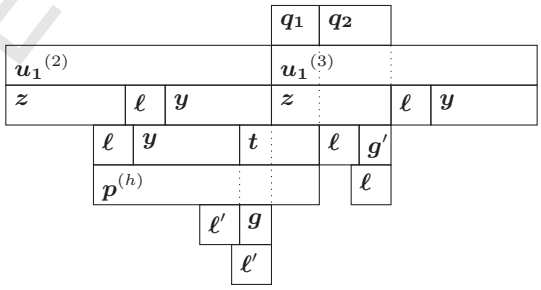


Fig. 14. Subcase 7 when (C1) holds and $g < 0$

(C2)

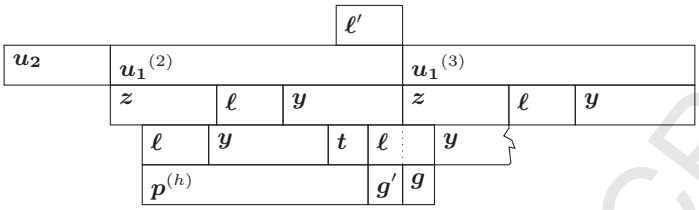


Fig. 15. Subcase 7 when (C2) holds

Suppose (C2) holds; that is, $\boldsymbol{t}$ is a substring of $\boldsymbol{y}$ and ends within distance $\boldsymbol{\ell}$ of the end of $\boldsymbol{y}$. By the periodicity of $\boldsymbol{u'}$, a prefix of $\boldsymbol{p} = \boldsymbol{\ell y t}$ follows $\boldsymbol{p}^{(h)}$. Let $\boldsymbol{g}$ be the suffix of $\boldsymbol{\ell}$ that overlaps $\boldsymbol{u_1}^{(3)}$, and let $\boldsymbol{g'}$ be the possibly empty prefix of $\boldsymbol{\ell}$ such that $\boldsymbol{\ell} = \boldsymbol{g'g}$. $\boldsymbol{\ell y}$ has period $t + g'$ because the suffix $\boldsymbol{\ell y}$ of $\boldsymbol{u_1}^{(2)}$ and the prefix $\boldsymbol{\ell y}$ of $\boldsymbol{p}^{(h)}$ are offset by length $t + g'$. $\boldsymbol{g'z}$ is a prefix of $\boldsymbol{\ell y}$ since, by assumption, $y \geqslant t + g' = z - g$.

$\boldsymbol{g'z}$ has period $t + g'$ as a prefix of $\boldsymbol{\ell y}$ and period ℓ as a suffix of $\boldsymbol{\ell' z}$, so by lemma 4 it has period $\gcd(t + g', \ell)$. Thus $\boldsymbol{\ell y}$ has period $t + g'$, and a prefix $\boldsymbol{g'z}$ of period $\gcd(t + g', \ell) \mid t + g'$, so $\boldsymbol{\ell y}$ has period $\gcd(t + g', \ell)$ by Lemma 6. Since $\boldsymbol{z\ell}$ has period ℓ and prefix $\boldsymbol{z}$ of period $\gcd(t + g', \ell) \mid \ell$, therefore by Lemma 6, $\boldsymbol{z\ell}$ has period $\gcd(t + g', \ell)$. $\boldsymbol{z\ell}$ and $\boldsymbol{\ell y}$ have period $\gcd(t + g', \ell)$ and share substring $\boldsymbol{\ell}$, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{z\ell y}$ has period $\gcd(t + g', \ell)$. Remarking that $\boldsymbol{\ell' t}$ and $\boldsymbol{\ell' t'}$ are both substrings of $\boldsymbol{u_1}$, we again conclude that $\boldsymbol{t} = \boldsymbol{t'}$.

(C3)

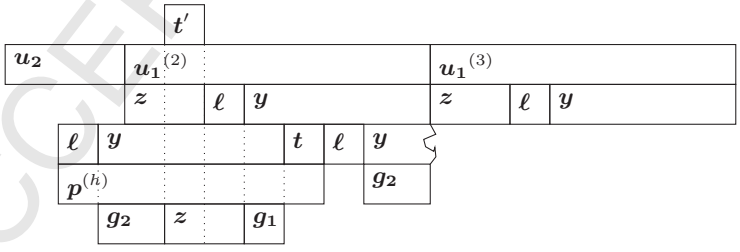


Fig. 16. Subcase 7 when (C3) holds

Suppose (C3) holds; that is, $\boldsymbol{t\ell}$ is a substring of $\boldsymbol{y}$. In this case, $\boldsymbol{z} = \boldsymbol{t'\ell}$ is also a substring of $\boldsymbol{y}$ because $y \geqslant t + \ell$ and the prefix $\boldsymbol{\ell y}$ of $\boldsymbol{p}^{(h)}$ ends at least z and at most y positions from the end of $\boldsymbol{u_1}^{(2)} = \boldsymbol{\ell' t' \ell y}$.

Let $\boldsymbol{g_1}$ and $\boldsymbol{g_2}$ be the (possibly empty) substrings of $\boldsymbol{y}$ immediately before and after $\boldsymbol{t\ell}$ such that $\boldsymbol{y} = \boldsymbol{g_1 t \ell g_2}$. Since $\boldsymbol{u_1 z}$ has period p, $\boldsymbol{g_1}$ and $\boldsymbol{g_2}$ are borders of $\boldsymbol{y}$ such that $\boldsymbol{y} = \boldsymbol{g_1 t \ell g_2} = \boldsymbol{g_2 t' \ell g_1}$.

Recall that $\boldsymbol{\ell'}$ is a suffix of $\boldsymbol{y}$, so $\boldsymbol{\ell'}$ is a suffix of $\boldsymbol{\ell g_2}$. Since the prefix $\boldsymbol{\ell g_2}$ of $\boldsymbol{p}$ occurs before the substring $\boldsymbol{z}$ of $\boldsymbol{y}$, $\boldsymbol{\ell'}$ also occurs before $\boldsymbol{z}$.

If $g_1 = g_2$, then $\boldsymbol{t}$ and $\boldsymbol{t'}$ occur at the same positions in two copies of $\boldsymbol{y}$, so that $\boldsymbol{t} = \boldsymbol{t'}$. If $g_1 \neq g_2$, several cases arise:

1. $g_1 < g_2$ $(g = g_2 - g_1)$

   Let $g = g_2 - g_1$, and let $\boldsymbol{g}$ be the nonempty prefix of $\boldsymbol{g_2}$ such that $\boldsymbol{g_2} = \boldsymbol{g g_1}$. $\boldsymbol{g_1}$ is a border of $\boldsymbol{g_2}$, so that $\boldsymbol{g_2}$ has period g.

   (a) $g \leqslant z$

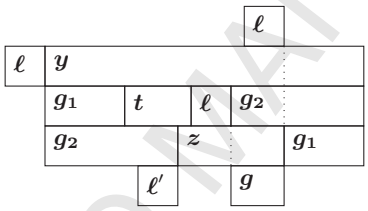


Fig. 17. Subcase 7 when (C3) holds, $g_1 < g_2$, and $g \leqslant z$

The proof requires several steps:

- As a suffix of $\boldsymbol{\ell' z}$, $\boldsymbol{\ell g}$ has period ℓ and suffix $\boldsymbol{\ell}$, hence border $\boldsymbol{\ell}$ and period g, therefore by Lemma 4 period $\gcd(g, \ell)$.
- Then $\boldsymbol{\ell' z}$ has period ℓ and a suffix $\boldsymbol{\ell g}$ of period $\gcd(g, \ell) \mid \ell$, so by Lemma 6, $\boldsymbol{\ell' z}$ has period $\gcd(g, \ell)$.
- Since $\boldsymbol{g_2}$ has period g and prefix $\boldsymbol{g}$ of period $\gcd(g, \ell) \mid g$, therefore by Lemma 6, $\boldsymbol{g_2}$ has period $\gcd(g, \ell)$.
- Since prefix $\boldsymbol{g_2}$ of $\boldsymbol{y}$ and $\boldsymbol{\ell' z}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{\ell'}$, therefore $\boldsymbol{g_2 z}$ has period $\gcd(g, \ell)$ by Lemma 5.
- Thus $\boldsymbol{t\ell}$ and $\boldsymbol{t'\ell}$ both have period $\gcd(g, \ell)$ as substrings of $\boldsymbol{g_2 z}$, implying that $\boldsymbol{t} = \boldsymbol{t'}$.

Note that $\boldsymbol{g_2 z}$ and $\boldsymbol{g_2}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{g}$, so that by Lemma 5, $\boldsymbol{y} = \boldsymbol{g_2 z g_1}$ has period $\gcd(g, \ell)$. Since $\boldsymbol{\ell g_2}$ has period $\gcd(g, \ell)$ as a substring of $\boldsymbol{y}$, and since $\boldsymbol{g_2}$ is a prefix of $\boldsymbol{y}$, therefore by Lemma 5, $\boldsymbol{\ell y}$ has period $\gcd(g, \ell)$. $\boldsymbol{z\ell} = \boldsymbol{\ell' z}$ and $\boldsymbol{\ell y}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{\ell}$, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{z\ell y}$ has period $\gcd(g, \ell)$.

(b) $g > z$

$\boldsymbol{y}$ has period $y - g_2 = z + g_1$, so $\boldsymbol{y}$ has a prefix $\boldsymbol{g_1 t \ell g_2'} = \boldsymbol{g_2' z g_1}$, where $\boldsymbol{g_2'}$ is a prefix of $\boldsymbol{g_2}$ and $|g_2' - g_1| \leqslant z$, so one of cases 1(a) and 2(a) applies.

2. $g_1 > g_2$ $(g = g_1 - g_2)$

Let $g = g' = g_1 - g_2$, let $\boldsymbol{g}$ be the nonempty suffix of $\boldsymbol{g_1}$ such that $\boldsymbol{g_1} = \boldsymbol{g_2 g}$, and let $\boldsymbol{g'}$ be the nonempty prefix of $\boldsymbol{g_1}$ such that $\boldsymbol{g_1} = \boldsymbol{g' g_2}$. Since $\boldsymbol{g_2}$ is a border of $\boldsymbol{g_1}$, therefore $\boldsymbol{g_1}$ and $\boldsymbol{g_2}$ have period $g = g'$.

(a) $g \leqslant z$

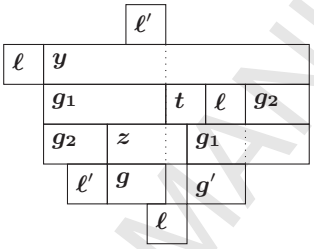


Fig. 18. Subcase 7 when (C3) holds, $g_1 > g_2$ and $g \leqslant z$

Again there are several steps:

- $\boldsymbol{\ell' g}$ has period ℓ as a prefix of $\boldsymbol{\ell' z}$ and shares suffix $\boldsymbol{\ell'}$ with $\boldsymbol{\ell g_1}$; accordingly, $\boldsymbol{\ell' g}$ has border $\boldsymbol{\ell'}$ and period g, hence periods g and ℓ, thus by Lemma 4 period $\gcd(g, \ell)$.
- $\boldsymbol{\ell' z}$ has period ℓ and prefix $\boldsymbol{\ell' g}$ of period $\gcd(g, \ell) \mid \ell$, hence by Lemma 6, it also has period $\gcd(g, \ell)$.
- $\boldsymbol{g_1}$ has period g and suffix $\boldsymbol{g}$ of period $\gcd(g, \ell) \mid g$, so again by Lemma 6, it also has period $\gcd(g, \ell)$.
- $\boldsymbol{g_1}$ and $\boldsymbol{\ell' z}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{g}$, so that by Lemma 5, $\boldsymbol{g_2 z}$ has period $\gcd(g, \ell)$.
- Prefix $\boldsymbol{\ell g'}$ of $\boldsymbol{\ell g_1}$ shares suffix $\boldsymbol{\ell}$ with $\boldsymbol{t\ell}$, so $\boldsymbol{\ell g'}$ has border $\boldsymbol{\ell}$ and period g. Moreover $\boldsymbol{\ell g'}$ has suffix $\boldsymbol{g'}$ which, as a prefix of $\boldsymbol{g_1}$, has period $\gcd(g, \ell) \mid g$, implying that $\boldsymbol{\ell g'}$ also has period $\gcd(g, \ell)$ by Lemma 6.
- $\boldsymbol{g_2 z}$ and $\boldsymbol{\ell g'}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{\ell}$, so by Lemma 5, $\boldsymbol{g_2 z g'}$ has period $\gcd(g, \ell)$.
- Then $\boldsymbol{g_2 z g'}$ and $\boldsymbol{g_1}$ have period $\gcd(g, \ell)$ and share substring $\boldsymbol{g'}$, so that by Lemma 5 the entire string $\boldsymbol{y} = \boldsymbol{g_2 z g_1}$ has period $\gcd(g, \ell)$.
- Therefore $\boldsymbol{t\ell}$ and $\boldsymbol{t'\ell}$ both have period $\gcd(g, \ell)$ as substrings of $\boldsymbol{y}$, so that $\boldsymbol{t} = \boldsymbol{t'}$, as required.

Since, as a substring of $\boldsymbol{y}$, $\boldsymbol{\ell g_1}$ has period $\gcd(g,\ell)$, and since $\boldsymbol{g_1}$ is also a prefix of $\boldsymbol{y}$, it follows from Lemma 5 that $\boldsymbol{\ell y}$ has period $\gcd(g,\ell)$. Note then that $\boldsymbol{z\ell} = \boldsymbol{\ell' z}$ and $\boldsymbol{\ell y}$ have period $\gcd(g,\ell)$ and share substring $\boldsymbol{\ell}$, so that by Lemma 5 $\boldsymbol{u_1} = \boldsymbol{z\ell y}$ has period $\gcd(g,\ell)$.

(b) $g > z$

$\boldsymbol{y}$ has period $y - g_1 = g_2 + z$, so $\boldsymbol{y}$ has a prefix $\boldsymbol{g_2 z g_1'} = \boldsymbol{g_1' t \ell g_2}$, where $\boldsymbol{g_1'}$ is a prefix of $\boldsymbol{g_1}$ and $|g_1' - g_2| \leqslant z$, so one cases 1(a) and 2(a) applies.

(C4)

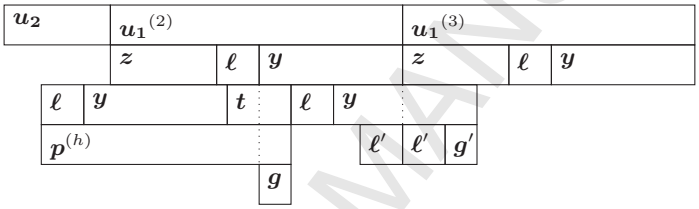


Fig. 19. Subcase 7 when (C4) holds

Suppose (C4) holds; that is, $\boldsymbol{t}$ begins to the left of $\boldsymbol{y}$ and ends inside it. Let $\boldsymbol{g}$ be the suffix of $\boldsymbol{t}$ that is also a prefix of $\boldsymbol{y}$. Let $\boldsymbol{g'}$ be the suffix of $\boldsymbol{y}$ of length $g' = g$. By the periodicity of $\boldsymbol{u'}$, a copy of $\boldsymbol{\ell y}$ follows $\boldsymbol{t}$, extending $\ell + g$ positions into $\boldsymbol{u_1}^{(3)}$. $\boldsymbol{\ell'}$ is a suffix of $\boldsymbol{\ell y}$, so $\boldsymbol{\ell'\ell' g'}$ is a suffix of $\boldsymbol{\ell y}$.

The suffix $\boldsymbol{\ell y}$ of $\boldsymbol{u_1}^{(2)}$ and the occurrence of $\boldsymbol{\ell y}$ that follows $\boldsymbol{t}$ are offset by length $\ell + g$, so $\boldsymbol{\ell y}$ has period $\ell + g$. Since $\boldsymbol{\ell'\ell' g'}$ has period $\ell + g$ as a suffix of $\boldsymbol{\ell y}$ and period ℓ as a prefix of $\boldsymbol{\ell' z}$, it therefore has period $\gcd(\ell + g, \ell) = \gcd(g, \ell)$ by Lemma 4. $\boldsymbol{\ell y}$ has period $\ell + g$ and suffix $\boldsymbol{\ell'\ell' g'}$ of period $\gcd(g,\ell) \mid \ell + g$, implying that it has period $\gcd(g,\ell)$ by Lemma 6. $\boldsymbol{z\ell}$ has period ℓ and substring $\boldsymbol{\ell}$ of period $\gcd(g,\ell) \mid \ell$, so by Lemma 6, it has period $\gcd(g,\ell)$. $\boldsymbol{z\ell}$ and $\boldsymbol{\ell y}$ have period $\gcd(g,\ell)$ and share substring ℓ, so by Lemma 5, $\boldsymbol{u_1} = \boldsymbol{z\ell y}$ has period $\gcd(g,\ell)$. Since $\boldsymbol{t\ell}$ and $\boldsymbol{t'\ell}$ are substrings of $\boldsymbol{u_1}$, we conclude finally that $\boldsymbol{t} = \boldsymbol{t'}$.

This completes the proof of Subcase 7. □

Lemma 12. *Suppose the conditions of Subcase 7 hold (Lemma 11). Then* $\boldsymbol{x} = \boldsymbol{d}^{x/d}$*, except possibly for*

(a) $v - u = (h-1)(u-w)$ **or**
(b) $v - u = (h - \frac{1}{2})(u-w)$,

where $d = \gcd(u,v,w)$ *and* $h = \left\lfloor \frac{u}{p} \right\rfloor$.

Proof. (All symbols used as defined in the proof of Lemma 11; refer to Figure 12.) Notice that in the proof of the lemma, $\boldsymbol{u_1}$ has period ℓ in all cases except when

(a′) (C1) holds and $g = 0$ **or**
(b′) (C3) holds and $g_1 = g_2$.

Suppose then that $\boldsymbol{u_1} = \boldsymbol{zr} = \boldsymbol{z\ell y}$ does indeed have period ℓ. Since $\boldsymbol{z} = \boldsymbol{\ell' t'}$ is a prefix of $\boldsymbol{u_1}$, it follows that $\boldsymbol{t'r} = \boldsymbol{t'\ell y}$ is a suffix of $\boldsymbol{u_1}$. Since $\boldsymbol{u_1}$ has period ℓ, $\boldsymbol{r} = \boldsymbol{\ell y}$ has prefix $\boldsymbol{y}$, and so $\boldsymbol{u_1}$ has border $\boldsymbol{t'\ell y}$ of length $p = t{+}\ell{+}y$, as therefore $\boldsymbol{u}$ does also. By Lemma 11, $\boldsymbol{u}$ has period p, so that by Lemma 9, $\boldsymbol{u} = \boldsymbol{u_1 u_2 u_1}$ has period $d_1 = \gcd(p, u_1 + u_2) = \gcd(u{-}w, v{-}u)$. Since $\boldsymbol{u}$ has a border of length p, it follows that $\boldsymbol{u}^2$ also has period d_1, as well as period u, so that by Lemma 4, $\boldsymbol{u}^2$ has period $\gcd(u, d_1) = \gcd(u, \gcd(u - w, v - u)) = \gcd(u, v, w) = d$. This periodicity clearly extends to all of $\boldsymbol{x}$.

Now consider the exceptional cases. For (a′), recall that in (C1) the gap g is the difference between the two prefixes of $\boldsymbol{x}$, $\boldsymbol{zp}^h$ and $\boldsymbol{u}$, where $p = u{-}w$, so that $g = 0$ implies $hp{+}z = u{+}t$. Substituting $z = k{+}w{-}u$, $t = k{-}u_1$ yields

$$h(u{-}w) = u{-}k{+}(u{-}w){+}k{-}u_1,$$

from which, with a little manipulation, (a) follows. For (b′), from Figure 16 $g_1 = g_2$ in (C3) implies

$$z{+}ph{-}t{-}(u_1{+}u_2{+}z{+}\ell) = u{-}(z{+}ph{+}\ell),$$

which since $z = \ell{+}t$ and $\ell = u_1{-}p$ becomes

$$2ph = u{+}u_1{+}u_2{-}u_1{+}p.$$

A bit more manipulation yields (b), completing the proof. □

5 General Case [eb]

In this section we present a sample lemma that considers three squares occurring close to each other, but with no two of them necessarily at the same position.

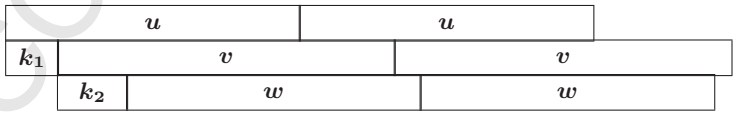


Fig. 20. $\boldsymbol{u^2}$ overlapping $\boldsymbol{v^2}$ (case (e)) that in turn overlaps $\boldsymbol{w^2}$ (case (b)): what is the combined effect?

According to our computational experiments, the following lemma applies to about three-quarters of cases in which the maximum alphabet size $\sigma = \gcd(u, v, w)$. Figure 20 illustrates case [*eb*].

Lemma 13. *In case* [*eb*]*, if* $k_2 \leqslant 2u - v - k_1 + d_1$*, then* $\boldsymbol{x}$ *has period* d*, where* $d = \gcd(u, v, w)$ *and* $d_1 = \gcd(v - u, v - w) = \gcd(u-w, v-w)$.

Proof. We use subscripts $_1$ to identify variables for $\boldsymbol{u}$ and $\boldsymbol{v}$, subscripts $_2$ for those of $\boldsymbol{v}$ and $\boldsymbol{w}$. Observe then that for $e_1 > 1,\ e_2 \geqslant 1$,

$$\boldsymbol{v} = \boldsymbol{p_1}^{e_1}\boldsymbol{k_1}\boldsymbol{p_1} = \boldsymbol{z_2}\boldsymbol{p_2}^{e_2},$$

where the variables subscripted $_1$ relate to case (e) of Lemma 8, those subscripted $_2$ to case (b). The substring $\boldsymbol{v'} = \boldsymbol{v}[z_2+1, v-k_1-p_1]$ has two periods, $p_1 = v-u$ and $p_2 = v - w$. To apply the Periodicity Lemma [11], we must have

$$\begin{aligned} p_1 + p_2 - \gcd(p_1, p_2) &\leqslant v - k_1 - p_1 - z_2 \\ k_2 &\leqslant 2u - v - k_1 + d_1 \end{aligned}$$

Thus if $k_2 \leqslant 2u-v-k_1+d_1$, then $\boldsymbol{v'}$ has period d_1. Moreover, $\boldsymbol{v}$ has a prefix of period p_1 that includes $\boldsymbol{v'}$, as well as a suffix of period p_2 that includes $\boldsymbol{v'}$, so $\boldsymbol{v}$ itself has period d_1. Since $\boldsymbol{p_1}$ is a border of $\boldsymbol{v}$, $\boldsymbol{v}$ is a repetition of period d_1. Because $\boldsymbol{u}$ is a substring of $\boldsymbol{v}^2$, $\boldsymbol{u}$ has period d_1. Therefore $\boldsymbol{x}$ has prefix $\boldsymbol{u}$ and suffix $\boldsymbol{v}^2$ both of period d_1 that include $\boldsymbol{v}[1..u-k_1]$. In case (e), $\frac{2(k_1+v)}{3} \leqslant u$ which implies $d_1 \leqslant u - k_1$, so $\boldsymbol{x}$ has period d_1. The substrings $\boldsymbol{u}^2$ and $\boldsymbol{w}^2$ then have periods $\gcd(d_1, u)$ and $\gcd(d_1, w)$, respectively, and so $\boldsymbol{x}$ itself has those periods. Finally, $\boldsymbol{x}$ has period $\gcd(d_1, u, w) = d$. □

The preceding lemma is a sample of the combinatorial information that may be obtained from considering all cases [ij] as specified above. To date, all the results given for the NPL in [9, 10, 30, 21, 13] deal only with the special cases $[ij]$, $i = a, d$, that arise for $k_1 = 0$.

6 Commentary & Future Research

The proofs of Lemmas 3 and 8 may, as indicated in the Introduction, open the way for new and more combinatorially sophisticated approaches to the bounding of the number of runs in any string of given length. Of course it would be highly desirable to find an approach to this lemma that would permit a much simplified and more suggestive proof.

In addition, much work remains to be done to state and prove results such as Lemma 13. In proving the results of [21], it turned out to be very helpful to look at the results of computer simulations for small values of k, u, v, w. It seems that similar techniques can profitably be used to generate conjectures for the cases $[ij]$ of three overlapping squares that arise from Lemma 8.

More generally, once the combinatorics of overlapping squares is well understood, it may well be possible to begin to design an algorithmic approach to the computation of runs that handles the various cases that arise without the need for elaborate preprocessing. This would for the first time permit direct analysis and computation of the local periodicities of a string in a manner consistent with their sparseness of occurrence.

Acknowledgements

This work was supported in part by the Natural Sciences & Engineering Research Council of Canada. The authors would like to thank two anonymous referees for their careful and constructive comments.

References

1. Alberto Apostolico & Franco P. Preparata, **Optimal off-line detection of repetitions in a string**, *Theoret. Comput. Sci. 22* (1983) 297–315.
2. Hideo Bannai, Tomohiro I, Shunsuke Inenaga, Yuto Nakashima, Masayuki Takeda & Kazuya Tsuruta, **The "Runs" Theorem**, `arXiv:1406.0263` (2014).
3. Gang Chen, Simon J. Puglisi & W. F. Smyth, **Fast & practical algorithms for computing all the runs in a string**, *Proc. 18th Annual Symp. Combinatorial Pattern Matching*, B. Ma & K. Zhang (eds.), LNCS 4580, Springer-Verlag (2007) 307–315.
4. Gang Chen, Simon J. Puglisi & W. F. Smyth, **Lempel-Ziv factorization using less time & space**, *Math. in Computer Science1–4* (2008) 605–623.
5. Maxime Crochemore, **An optimal algorithm for computing all the repetitions in a word**, *Inform. Process. Lett. 12–5* (1981) 244–248.
6. Maxime Crochemore & Lucian Ilie, **Maximal repetitions in strings**, *J. Comput. Sys. Sci.* (2008) 796–807.
7. Maxime Crochemore, Lucian Ilie & Liviu Tinta, **Towards a solution to the "runs" conjecture**, *Proc. 19th Annual Symp. Combinatorial Pattern Matching*, P. Ferragina & G. Landau (eds.), LNCS 5029, Springer-Verlag (2008) 290–302.
8. Maxime Crochemore, Lucian Ilie & Liviu Tinta, **The "runs" conjecture**, *TCS 412–27* (2011) 2931–2941.
9. Maxime Crochemore and Wojciech Rytter, **Squares, cubes, and time-space efficient strings searching**, *Algorithmica 13* (1995) 405–425.
10. Kangmin Fan, Simon J. Puglisi, W. F. Smyth & Andrew Turpin, **A new periodicity lemma**, *SIAM J. Discrete Math. 20–3* (2006) 656–668.
11. N. J. Fine and H. S. Wilf, **Uniqueness theorems for periodic functions**, *Proc. Amer. Math. Soc. 16* (1965) 109–114.
12. Aviezri S. Fraenkel & Jamie Simpson, **The exact number of squares in Fibonacci words**, *Theoret. Comput. Sci. 218–1* (1999) 95–106.
13. Frantisek Franek, Robert C. G. Fuller, Jamie Simpson & W. F. Smyth, **More results on overlapping squares**, *J. Discrete Algorithms 17* (2012) 2–8.
14. Frantisek Franek & Q. Yang, **An asymptotic lower bound for the maximal number of runs in a string**, *Internat. J. Foundations of Computer Science19–1* (2008) 195–203.
15. Frantisek Franek, R. J. Simpson & W. F. Smyth, **The maximum number of runs in a string**, *Proc. 14th Australasian Workshop on Combinatorial Algs.*, Mirka Miller & Kunsoo Park (eds.) (2003) 26–35.
16. Mathieu Giraud, **Not so many runs in strings**, *Proc. 2nd Internat. Conf. on Language & Automata Theory & Applications*, Carlos Martín-Vide, Friedrich Otto & Henning Fernau (eds.), LNCS 5196, Springer-Verlag (2008) 232–239.
17. Mathieu Giraud, **Asymptotic behavior of the numbers of runs and microruns**, *Inform. & Computation* 207–11 (2009) 1221–1228.

18. Costas S. Iliopoulos & W. F. Smyth, **A characterization of the squares in a Fibonacci string**, *Theoret. Comput. Sci.* 172 (1997) 281–291.
19. Roman Kolpakov & Gregory Kucherov, **On maximal repetitions in words**, *J. Discrete Algorithms 1* (2000) 159–186.
20. Kazuhiko Kusano, Kazuyuki Narisawa & Ayumi Shinohara, **On morphisms generating run-rich strings**, *Proc. Prague Stringology Conf.2013* (2013) 35–47.
21. Evguenia Kopylova & W. F. Smyth, **The three squares lemma revisited**, *J. Discrete Algorithms 11* (2012) 3–14.
22. M. Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press (2002) 504 pp.
23. Michael G. Main, **Detecting leftmost maximal periodicities**, *Discrete Applied Maths. 25* (1989) 145–153.
24. Michael G. Main & Richard J. Lorentz, **An $O(n \log n)$ algorithm for finding all repetitions in a string**, *J. Algorithms 5* (1984) 422–432.
25. Wataru Matsubara, Kazuhiko Kusano, Akira Ishino, Hideo Bannai & Ayumi Shinohara, **New lower bounds for the maximum number of runs in a string**, *PSC* (2008) 140–145.
26. Simon J. Puglisi & R. J. Simpson, **The expected number of runs in a word**, *Australasian J. Combinatorics 42* (2008) 45–54.
27. Simon J. Puglisi, R. J. Simpson & W. F. Smyth, **How many runs can a string contain?**, *Theoret. Comput. Sci. 401* (2008) 165–171.
28. Wojciech Rytter, **The number of runs in a string: improved analysis of the linear upper bound**, *Proc.* 23rd *Symp. Theoretical Aspects of Computer Science*, B. Durand & W. Thomas (eds.), LNCS 2884, Springer-Verlag (2006) 184–195.
29. SHARCNET, `https://www.sharcnet.ca/my/front/`
30. R. J. Simpson, **Intersecting periodic words**, *Theoret. Comput. Sci.* 374 (2007) 58–65.
31. Jamie Simpson, **Modified Padovan words and the maximum number of runs in a word**, *Australasian J. Combinatorics* 46 (2010) 129–145.
32. Bill Smyth, *Computing Patterns in Strings*, Pearson Addison-Wesley (2003) 423pp.