# Non-Rectangular Convolutions and (Sub-)Cadences with Three Elements

**Mitsuru Funakoshi**
Department of Informatics, Kyushu University, Japan
mitsuru.funakoshi@inf.kyushu-u.ac.jp

**Julian Pape-Lange**
Technische Universität Chemnitz, Straße der Nationen 62, 09111 Chemnitz, Germany
julian.pape-lange@informatik.tu-chemnitz.de

## Abstract

The discrete acyclic convolution computes the $2n + 1$ sums

$$\sum_{\substack{i+j=k \\ (i,j)\in[0,1,2,\ldots,n]^2}} a_i b_j$$

in $\mathcal{O}(n \log n)$ time. By using suitable offsets and setting some of the variables to zero, this method provides a tool to calculate all non-zero sums

$$\sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_i b_j$$

in a rectangle $P$ with perimeter $p$ in $\mathcal{O}(p \log p)$ time.

This paper extends this geometric interpretation in order to allow arbitrary convex polygons $P$ with $k$ vertices and perimeter $p$. Also, this extended algorithm only needs $\mathcal{O}\left(k + p(\log p)^2 \log k\right)$ time.

Additionally, this paper presents fast algorithms for counting sub-cadences and cadences with 3 elements using this extended method.

**2012 ACM Subject Classification** Mathematics of computing → Combinatorial algorithms; Mathematics of computing → Combinatorics on words; Theory of computation → Computational geometry; Computing methodologies → Number theory algorithms

**Keywords and phrases** discrete acyclic convolutions, string-cadences, geometric algorithms, number theoretic transforms

**Digital Object Identifier** 10.4230/LIPIcs.STACS.2020.30

**Related Version** The preprint of this paper can be found at `https://arxiv.org/abs/1910.11564`.

**Acknowledgements** The first author discovered an error in the algorithm for determining the existence of 3-cadences in "String cadences" of Amir et al., which led to false positives. After that, the first author reported this error to Travis Gagie, one of the authors of "String Cadences". Travis Gagie explained this error to the second author during the 30th Annual Symposium on Combinatorial Pattern Matching (CPM 2019) in Pisa. He also claimed that it should be possible to determine the existence of 3-cadences in sub-quadratic time. Juliusz Straszyński showed during the same conference that 3-sub-cadences beginning and ending in given intervals can efficiently be detected by convolution. Amihood Amir noted later in an email that we can also efficiently count these sub-cadences, which allows "subtractive" methods as used for arbitrary triangles.







## 1 Introduction

The convolution is a well-known and very useful method, which is not only closely linked to signal processing (e.g. [18]) but is also used to multiply polynomials (see [5, p. 905]) and large numbers (e.g. [17] (written in German)) in quasi-linear time. The convolution can be efficiently computed with the fast Fourier transform or its counterpart in residue class rings, the number theoretic transform:

▶ **Theorem 1.** *Let $a = (a_0, a_1, a_2, \ldots, a_n)$ and $b = (b_0, b_1, b_2, \ldots, b_n)$ be two sequences. The sequence $c = (c_0, c_1, c_2, \ldots, c_{2n})$ with $c_k = \sum_{i+j=k} (a_i b_j)$ can be computed in $\mathcal{O}(n \log n)$ operations.*

The most well-known proofs use additions and multiplications of arbitrary complex numbers. However, with the finite register lengths of real-world computers, one must either cope with the roundoff errors or do all calculations in a different ring. In Appendix A, we show that a suitable ring can be found deterministically in $\mathcal{O}\left(n(\log n)^2(\log\log n)\right)$ time if the generalized Riemann hypothesis is true.

The convolution can also be interpreted geometrically: Let $a = (a_0, a_1, a_2, \ldots, a_n)$ and $b = (b_0, b_1, b_2, \ldots, b_n)$ be sequences. Then the convolution calculates the partial sums

$$\sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_i b_j,$$

where $P$ is the square given by $\{(x, y) : 0 \leq x, y \leq n\}$.

This paper extends this geometric interpretation and shows that if $P$ is an arbitrary convex polygon with $k$ vertices and perimeter $p$, the partial sums can be calculated in $\mathcal{O}\left(k + p(\log p)^2 \log k\right)$ time.

We also use this extended method to solve an open problem of a string pattern called cadence. A cadence is given by an arithmetic progression of occurrences of the same character in a string such that the progression cannot be extended to either side without extending the string as well. For example, in the string 001001001 the indices $(3, 6, 9)$ corresponding to the "1"s form a 3-cadence. On the other hand, in the string 001010100 the indices $(3, 5, 7)$ corresponding to the "1"s do not form a 3-cadence since, for example, the index 1 is still inside of the string.

3-cadences can be found naïvely in quadratic time. In the paper [2], a quasi-linear time algorithm for detecting the existence of 3-cadences was proposed, but this algorithm also detects false positives as the aforementioned string 001010100.

This paper fixes this issue and also extends the algorithm to the slightly more general notion of $(a, b, c)$-partial-$k$-cadences. The resulting extended algorithm also allows counting those partial-cadences with a given character of an alphabet $\Sigma$ of a string with length $n$ and only needs $\mathcal{O}\left(n(\log n)^2\right)$ time. Using a method presented by Amir et al. in [2], this implies that all $(a, b, c)$-partial-$k$-cadences can be counted in $\mathcal{O}\left(\min(|\Sigma|n(\log n)^2, n^{3/2}\log n)\right)$ time.

Furthermore, we show that the output of the counting algorithm also allows finding $x$ partial-cadences in $\mathcal{O}(xn)$ time.

This paper also gives similar results for 3-sub-cadences.

For the time complexity, we assume that arithmetic operations with $\mathcal{O}(\log n)$ bits can be done in constant time. In particular, we want to be able to get the remainder of a division by a prime $p < 2(2n\log(2n))^2$ in constant time.

Also, in this paper, we assume a suitable alphabet. I.e. the characters are given by sufficiently small integers in order to allow constant time reading of a given character in the string and in order to allow sorting the characters.

## 2 (Sub-)Cadences and Their Definitions

While the concept of cadences in the context of strings was already considered in [19] by Van der Waerden, the term cadence dates back to 1964 and was first introduced by Gardelle and Guilbaud in [8] (written in French). Since then, there were at least two other, slightly different and non-equivalent definitions given by Lothaire in [15, Chapter 3.3] and Amir et al. in [2].

This paper uses the most restrictive definition of the cadence, which was introduced by Amir et al. in [2], and also uses their definition of the sub-cadence, which is equivalent to Gardelle's cadence in [8] and Lothaire's arithmetic cadence in [15, Chapter 3.3].

A string $S$ of length $n$ is the concatenation $S = S[1..n] = S[1]S[2]S[3]\dots S[n]$ of characters from an alphabet $\Sigma$.

▶ **Definition 2.** *A* $k$-sub-cadence *is a triple* $(i, d, k)$ *of positive integers such that*

$$S[i] = S[i+d] = S[i+2d] = \dots = S[i+(k-1)d]$$

*holds.*

In this paper, cadences are additionally required to start and end close to the boundaries of the string:

▶ **Definition 3.** *A* $k$-cadence *is a* $k$*-sub-cadence* $(i, d, k)$ *such that the inequalities* $i - d \leq 0$ *and* $n < i + kd$ *hold.*

Since for any $k$-sub-cadence the inequality $i + (k-1)d \leq n$ holds, for any $k$-cadence $i + (k-1)d \leq n < i + kd$ holds. This implies $k - 1 \leq \frac{n-i}{d} < k$ and thereby $k = \lfloor \frac{n-i}{d} \rfloor + 1$. It is therefore sufficient to omit the variable $k$ of a $k$-cadence $(i, d, k)$ and just denote this $k$-cadence by the pair $(i, d)$.

▶ Remark 4 (Comparison of the Definitions).

- The cadence as defined by Lothaire is just an ordered sequence of unequal indices such that the corresponding characters are equal.
- The cadence as defined by Gardelle and Guilbaud additionally requires the sequence to be an arithmetic sequence.
- The cadence as defined by Amir et al. and as used in this paper additionally requires that the cadence cannot be extended in any direction without extending the string as well.

For the analysis of cadences with errors, we need two more definitions:

▶ **Definition 5.** *A* $k$-cadence with at most $m$ errors *is a tuple* $(i, d, k, m)$ *of integers such that* $i, d, k \geq 1$ *and* $i - d \leq 0$ *and* $n < i + kd$ *hold and such that there are* $k - m$ *different integers* $\pi_j \in \{0, 1, 2, \dots, k-1\}$ *with* $j = 1, 2, 3, \dots, k - m$ *and*

$$S[i + \pi_1 d] = S[i + \pi_2 d] = S[i + \pi_3 d] \dots = S[i + \pi_{k-m} d].$$

A particularly interesting case of cadences with errors is given by the partial-cadences in which we know all positions where an error is allowed:

▶ **Definition 6.** *For some different integers* $\pi_j \in \{0, 1, 2, \dots, k-1\}$ *with* $j = 1, 2, 3, \dots, p$, *a* $(\pi_1, \pi_2, \pi_3, \dots, \pi_p)$-partial-$k$-cadence *is a triple* $(i, d, k)$ *of positive integers with* $i - d \leq 0$ *and* $n < i + kd$ *such that*

$$S[i + \pi_1 d] = S[i + \pi_2 d] = S[i + \pi_3 d] \dots = S[i + \pi_p d]$$

*hold.*

In this paper, we will only consider the case of $k - 3$ errors. I.e. $k$*-cadences with at most* $k - 3$ *errors* and $(a, b, c)$*-partial-*$k$*-cadences* for three different integer $a, b, c \in \{0, 1, ..., k-1\}$.

## 3 3-Sub-Cadences and Rectangular Convolutions

It is a direct consequence of van der Waerden's theorem that sufficiently large strings are guaranteed to have sub-cadences of a given length:

▶ **Theorem 7** (Existence of sub-cadences (Van der Waerden [19] (written in German), see Lothaire [15, Chapter 3.3])).

*Let $\Sigma$ be an alphabet and $k$ an integer. There exists an integer $N = N(|\Sigma|, k)$ such that every string containing at least $N$ characters has at least one $k$-sub-cadence*

However, this theorem does not provide the number of $k$-sub-cadences of a given string.

In this section, we will show that 3-sub-cadences with a given character of a string of length $n$ can be efficiently counted in $\mathcal{O}(n \log n)$ time. We will also show that arbitrary 3-sub-cadences of a string of length $n$ can be counted in $\mathcal{O}\left(n^{3/2}(\log n)^{1/2}\right)$ time and that both counting algorithms allow us to output $x$ different 3-sub-cadences in $\mathcal{O}(xn)$ additional time if at least $x$ different 3-sub-cadences exist.

Let $\sigma \in \Sigma$ be a character. We will now count all 3-sub-cadences with character $\sigma$.

Let $(i, d)$ be a 3-sub-cadence. Since $i + d = \frac{i+(i+2d)}{2}$ holds, the position $i + d$ of the middle occurrence of $\sigma$ only depends on the sum of the index $i$ of first occurrence and the index $i + 2d$ of the third occurrence but does not depend on the individual indices of those two positions. Therefore, it is possible to determine the candidates for the middle occurrences with the convolution of the candidates of the first occurrence and the candidates of the third occurrence.

Let the sequence $\delta = (\delta_0, \delta_1, \delta_2, \ldots, \delta_n)$ be given by the indicator function for $\sigma$ in $S$:

$$\delta_i := \begin{cases} 1 & \text{if } S[i] = \sigma \\ 0 & \text{if } S[i] \neq \sigma \text{ (this includes } i = 0) \end{cases}$$

With this definition, the product $\delta_i \delta_j$ is 1 if and only if $S[i] = S[j] = \sigma$ and otherwise is 0. Therefore $c_k = \sum_{i+j=k} (\delta_i \delta_j) = \#\{i : S[i] = S[k - i] = \sigma\}$ counts in how many ways the index $\frac{k}{2}$ lies in the middle of two $\sigma$. These partial sums can be calculated in $\mathcal{O}(n \log n)$ time by convolution.

If $k$ is odd or $S\left[\frac{k}{2}\right] \neq \sigma$ holds, the index $\frac{k}{2}$ cannot be the middle index of a 3-sub-cadence. If $S\left[\frac{k}{2}\right] = \sigma$ holds, the indicator function $\delta_{\frac{k}{2}}$ is 1, and therefore $\delta_{\frac{k}{2}} \delta_{\frac{k}{2}} = 1$ holds as well. Since the arithmetic progression $(\delta_{\frac{k}{2}}, 0, 3)$ consisting of three times the number $\delta_{\frac{k}{2}}$ is not a 3-sub-cadence, the output element $c_k$ contains one false positive. Additionally, for $i + j = k$ with $i \neq j$ and $S[i] = S[j] = \sigma$, the output element $c_k$ counts the combination $\delta_i \delta_j$ as well as $\delta_j \delta_i$.

Therefore,

$$s_k := \begin{cases} \frac{c_{2k}-1}{2} & \text{if } S[k] = \sigma \\ 0 & \text{if } S[k] \neq \sigma \end{cases}$$

counts exactly the number of 3-sub-cadences with character $\sigma$ such that the second occurrence of $\sigma$ has index $k$. The sum of the $s_k$ is the number of total 3-sub-cadences with character $\sigma$.

Also, for each $s_k \neq 0$, all those $s_k$ 3-sub-cadences can be found in $\mathcal{O}(k) \subseteq \mathcal{O}(n)$ time by checking for each index $i < k$ whether $S[i] = S[k] = S[2k - i] = \sigma$ holds.

If the character $\sigma$ is rare, we can also follow the idea of Amir et al. in [2] for detecting 3-cadences with rare characters: If all $n_\sigma$ occurrences of the character are known, the $c_k$ can be computed in $\mathcal{O}(n_\sigma^2)$ time by computing every pair of those occurrences. Therefore:

▶ **Theorem 8.** *For every character $\sigma \in \Sigma$, the 3-sub-cadences with $\sigma$ can be counted in $\mathcal{O}(n \log n)$ time. Also, if all $n_\sigma$ occurrences of $\sigma$ are known, the 3-sub-cadences with $\sigma$ can be counted in $\mathcal{O}(n_\sigma^2)$ time.*

Following the proof in [2], we can get all occurrences of every character by sorting the input string in $\mathcal{O}(n \log n)$ time. This implies that the algorithm needs at most $\mathcal{O}\left(\sum_{\sigma\in\Sigma} \min(n_\sigma^2, n \log n)\right) \subseteq \mathcal{O}\left(\frac{n}{(n\log n)^{1/2}} n \log n\right) = \mathcal{O}(n^{3/2}(\log n)^{1/2})$ time.

▶ **Theorem 9.** *The number of all 3-sub-cadences can be counted in*

$$\mathcal{O}\left(\min(|\Sigma| n \log n, n^{3/2}(\log n)^{1/2})\right) \text{ time.}$$

▶ **Theorem 10.** *After counting at least $x$ 3-sub-cadences, it is possible to output $x$ 3-sub-cadences in $\mathcal{O}(xn)$ time.*

## 4 Non-Rectangular Convolutions

In this section, we will extend the geometric interpretation of the convolution and show that for convex polygons $P$ with $k$ vertices and perimeter $p$ it is possible to calculate the partial sums

$$c_k = \sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_i b_j$$

in $\mathcal{O}\left(k + p(\log p)^2 \log k\right)$ time.

Let us imagine a graph where all integer coordinates $(i, j)$ have the value $f(i, j) := a_i b_j$. We do not need the convolution in order to determine the sum of the function values in a given rectangle since we can use the simple factorization $\sum_{i=0}^{n}\sum_{j=0}^{m}(a_i b_j) = \left(\sum_{i=0}^{n} a_i\right)\left(\sum_{j=0}^{m} b_j\right)$ in $\mathcal{O}(n+m)$ time. However, the convolution provides the $2n$ partial sums on the 45°-diagonals in almost the same time of $\mathcal{O}((n + m)\log(n + m))$.

We will now extend this geometric interpretation firstly to triangles with a vertical cathetus and a horizontal cathetus, then to arbitrary triangles and lastly to convex polygons. In order to do this, we will cover the given polygon $P$ in polygons $P_p^+$ and $P_m^-$ such that for each integer point $(i, j)$ the equality

$$\#\{P_p^+ | (i,j) \in P_p^+\} - \#\{P_m^- | (i,j) \in P_m^-\} = \begin{cases} 1 & \text{if } (i,j) \in P \\ 0 & \text{if } (i,j) \notin P \end{cases}$$

holds, and we define

$$(c_p)_k := \sum_{\substack{i+j=k \\ (i,j)\in P_p^+\cap\mathbb{Z}^2}} a_i b_j \text{ and } (c_m)_k := -\sum_{\substack{i+j=k \\ (i,j)\in P_m^-\cap\mathbb{Z}^2}} a_i b_j.$$

By construction, $c_k = (\sum(c_p)_k) + (\sum(c_m)_k)$ holds. However, if the edges and vertices of the polygons $P_p^+$ and $P_m^-$ contain integer points, we need to carefully decide for every of these polygons, which edges and vertices are supposed to be included in the polygons and which are excluded from the polygons.

▶ **Lemma 11.** *Let $P$ be a triangle with a vertical cathetus and a horizontal cathetus and perimeter $p$. Let also the sequences $a = (a_0, a_1, a_2, \ldots, a_n)$ and $b = (b_0, b_1, b_2, \ldots, b_n)$ be given.*

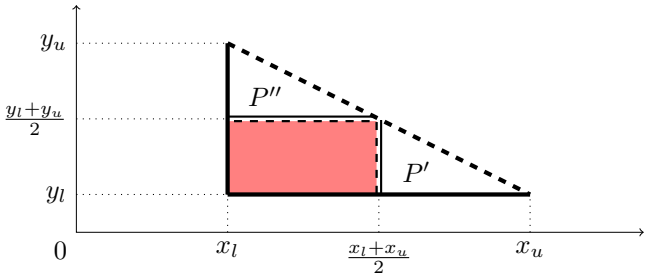


**Figure 1** The right-angled triangle $P$ in Lemma 11.

*Then the partial sums*

$$c_k = \sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_i b_j$$

*can be calculated in* $\mathcal{O}\left(p(\log p)^2\right)$ *time.*

**Proof.** The proof will be symmetrical with regard to horizontal and vertical mirroring. Therefore, without loss of generality, we will assume that $P$ is oriented as in Figure 1.

We first initialize the output vector $c = (c_{x_l+y_l}, c_{x_l+y_l+1}, c_{x_l+y_l+2}, \ldots, c_{x_u+y_u})$ with zero. This takes $\mathcal{O}(p)$ time.

In the following proof, we assume that both catheti are included in the polygon and that the hypotenuse as well as its endpoints are excluded. If this is not the expected behavior, we can traverse the edges in $\mathcal{O}(p)$ time and for each integer point $(i, j)$ on the edge, we can decrease/increase the corresponding $c_{i+j}$ by $a_i b_j$ if necessary.

If $p$ is at most one, there is at most one integer point $(i, j)$ in the triangle, and this point can be found in constant time. In this case, we only have to increase $c_{i+j}$ by $a_i b_j$.

If $p$ is bigger than one, we will separate the triangle $P$ into three disjoint parts as seen in Figure 1.

- The triangle $P'$ of points with x-coordinate of at least $\left\lceil \frac{x_l+x_u}{2} \right\rceil$,
- the triangle $P''$ of points with y-coordinate of at least $\left\lceil \frac{y_l+y_u}{2} \right\rceil$ and
- the red rectangle of points with x-coordinate of at most $\left\lceil \frac{x_l+x_u}{2} \right\rceil - 1$ and y-coordinate of at most $\left\lceil \frac{y_l+y_u}{2} \right\rceil - 1$.

There are no integers bigger than $\left\lceil \frac{x_l+x_u}{2} \right\rceil - 1$ but smaller than $\left\lceil \frac{x_l+x_u}{2} \right\rceil$ nor integers bigger than $\left\lceil \frac{y_l+y_u}{2} \right\rceil - 1$ but smaller than $\left\lceil \frac{y_l+y_u}{2} \right\rceil - 1$. Therefore, each integer point in $P$ is in exactly one of the three parts.

For the red rectangle, we can calculate the convolution and thereby get the corresponding partial sums in $\mathcal{O}(p \log p)$ time. The partial sums corresponding to the sub-triangles are calculated recursively. Increasing the $c_k$ by the partial results leads to the final result.

Hence, the algorithm takes

$$\mathcal{O}\left(p + \left(\sum_{i=0}^{\log_2 p} 2^i \left(\frac{p}{2^i} \log \frac{p}{2^i}\right)\right) + 2^{\log_2 p}\right) \subseteq \mathcal{O}\left(\sum_{i=0}^{\log p} p \log p\right) = \mathcal{O}\left(p(\log p)^2\right)$$

time. ◀

We will now further extend this result to arbitrary triangles:

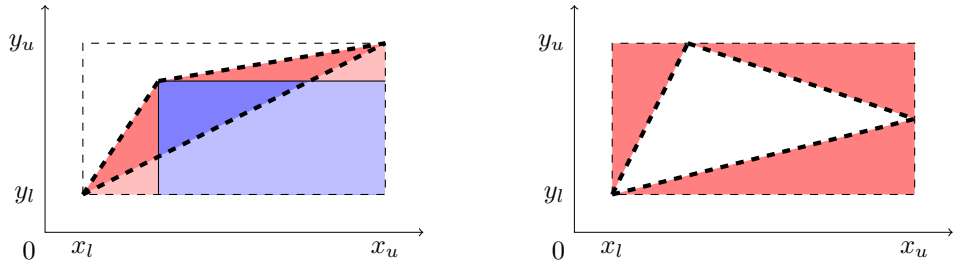


**Figure 2** The two possible triangles $P$ in Lemma 12.

▶ **Lemma 12.** *Let a triangle $P$ with perimeter $p$ and sequences $a = (a_0, a_1, a_2, \ldots, a_n)$ and $b = (b_0, b_1, b_2, \ldots, b_n)$ be given.*

*Then the partial sums*

$$c_k = \sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_i b_j$$

*can be calculated in $\mathcal{O}\left(p(\log p)^2\right)$ time.*

**Proof.** Let $x_l, y_l, x_u, y_u$ be the minimal and maximal x-coordinates and y-coordinates of the three vertices of the polygon $P$. As in the last lemma, we first initialize the output vector $c = (c_{x_l+y_l}, c_{x_l+y_l+1}, c_{x_l+y_l+2}, \ldots, c_{x_u+y_u})$.

Similarly to the last lemma, we can remove/add edges and vertices in linear time with respect to $p$. Since the number of edges and vertices is constant, we ignore them for the sake of simplicity.

Let $R$ be the rectangle $\{(x, y)|x_l < x < x_u \wedge y_l < y < y_u\}$. Since $R$ has four edges but $P$ only has three vertices, at least one of the vertices of $P$ is also a vertex of $R$. Without loss of generality, this vertex is $(x_l, y_l)$.

**Case 1:** The opposing vertex $(x_u, y_u)$ in $R$ also coincides with a vertex of $P$ (as in the left-hand side of Figure 2):

Without loss of generality, we can assume that the third vertex of $P$ is above the diagonal from $(x_l, y_l)$ to $(x_u, y_u)$. In this case, the partial sums corresponding to $P$ are given by the sum of the partial sums of the red triangles and the partial sums of the blue rectangle minus the partial sums of the lighter triangle.

There are only three triangles and one rectangle involved, and each of those polygons has perimeter $\mathcal{O}(p)$. Furthermore, all triangles have a vertical cathetus and a horizontal cathetus. Therefore, using Lemma 11, we can calculate all partial sums in $\mathcal{O}\left(p(\log p)^2\right)$ time.

**Case 2:** The opposing vertex $(x_u, y_u)$ in $R$ does not coincide with a vertex of $P$ (as in the right-hand side of Figure 2):

In this case, one vertex of $P$ lies on the right edge of $R$ and one vertex of $P$ lies on the upper edge of $R$.

The wanted partial sums are in this case the difference of the partial sums of the rectangle and of the partial sums of the three red triangles. Again, we can calculate all partial sums in $\mathcal{O}\left(p(\log p)^2\right)$ time.

Since both cases require $\mathcal{O}\left(p(\log p)^2\right)$ time, this concludes the proof. ◀

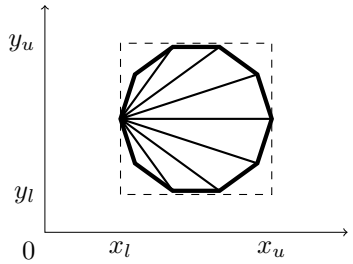


**Figure 3** A regular $k$-gon. All chords from the leftmost vertex to the vertices on the right-hand side of the $k$-gon are at least $\frac{p}{4}$ long. The sum of all chords' lengths is therefore $\Theta(kp)$.

Now we will extend this algorithm to convex polygons with $k$ vertices by dissecting them into $k-2$ triangles by adding $k-3$ chords. Since the time complexity of the triangular convolution given by Lemma 12 depends on the sum of the triangles' perimeters, it is not sufficient to just select one vertex and connect it with every other vertex in the polygon (see Figure 3). On the other hand, the triangulation algorithm itself should not take longer than the convolutions. Additionally, the order in which the chords are added does not matter for the convolutions. We will show that for convex polygons there is a triangulation which can be computed in linear time and only increases the perimeter by the factor $\mathcal{O}(\log k)$.

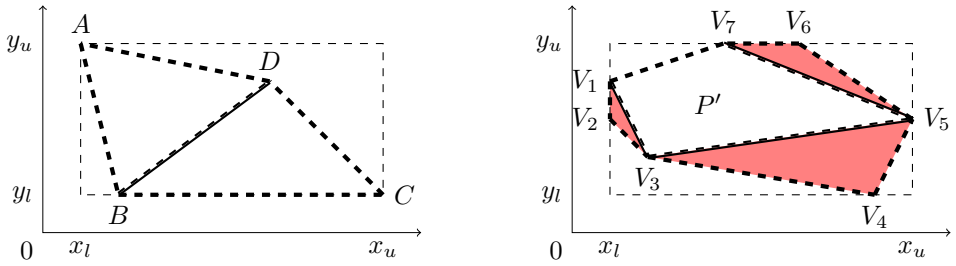


**Figure 4** Two possible convex polygons $P$ with more than 3 vertices in Lemma 13.

▶ **Theorem 13.** *Let $P$ be a convex polygon with $k$ vertices and perimeter $p$. Let also the sequences $a = (a_0, a_1, a_2, \ldots, a_n)$ and $b = (b_0, b_1, b_2, \ldots, b_n)$ be given.*

*Then the partial sums*

$$c_k = \sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_i b_j$$

*can be calculated in $\mathcal{O}\left(k + p(\log p)^2 \log k\right)$ time.*

**Proof.** As in the last two Lemmata, we define $x_l, y_l, x_u, y_u$ to be the minimal and maximal x-coordinates and y-coordinates of the $k$ vertices of $P$. Also, we first initialize the output vector $c = (c_{x_l+y_l}, c_{x_l+y_l+1}, c_{x_l+y_l+2}, \ldots, c_{x_u+y_u})$. We further assume that none of the edges and vertices of $P$ is included in $P$.

If $P$ is a triangle, then this Lemma simplifies to Lemma 12 and there is nothing left to prove.

If $P$ is a quadrilateral $ABCD$, as in the left-hand side of Figure 4, then it can be partitioned into the triangles $ABD$ and $CDB$ where the edge $BD$ is included in exactly one triangle and all other edges are excluded. The triangle inequality proves that $|BD| \leq |DA| + |AB|$ and $|BD| \leq |BC| + |CD|$ hold. Therefore, both triangles have a perimeter of at most $p$. This implies that the partial sums can be calculated in $\mathcal{O}\left(p(\log p)^2\right)$.

If $P$ is a polygon $V_1V_2V_3\dots V_k$ with more than four vertices, as in the right-hand side of Figure 4, it can be partitioned into

- the polygon $P' = V_1V_3V_5\dots V_{2\lceil\frac{k}{2}\rceil-1}$, which is given by the odd vertices without its edges,
- the red triangles $V_iV_{i+1}V_{i+2}$ with $i = 1, 3, 5, \dots, 2\left\lceil\frac{k}{2}\right\rceil - 3$ including the edge $V_iV_{i+2}$ but excluding the other edges and the vertices,
- if $k$ is even, the triangle $V_{k-1}V_k$ including the edge $V_{k-1}V_{k+1}$ but excluding the other edges and the vertices.

By construction and triangle inequality, the perimeter $p'$ of $P'$ is at most $p$. This, however, also implies that the total perimeter $\sum p_i$ of the triangles is at most $2p$. The inequality

$$\sum \min\left(1, p_i(\log p_i)^2\right) \leq k + \sum \left(p_i(\log p)^2\right) \leq k + p(\log p)^2$$

implies that the algorithm needs $\mathcal{O}\left(k + p(\log p)^2\right)$ time plus the time we need for processing $P'$. Since each step almost halves the number of vertices, we need $\mathcal{O}(\log k)$ steps. This results in a total time complexity of $\mathcal{O}\left(k + p(\log p)^2 \log k\right)$. ◀

## 5 (a,b,c)-Partial-k-Cadences

In this section, we will show how the non-rectangular convolution helps counting the $(a, b, c)$-partial-$k$-cadences as defined in Definition 6.

In particular, we will show that $(a, b, c)$-partial-$k$-cadences with a given character $\sigma$ can be counted in $\mathcal{O}\left(n(\log n)^2\right)$ time. We will further show that all $(a, b, c)$-partial-$k$-cadences can be counted in $\mathcal{O}\left(\min(|\Sigma|n(\log n)^2, n^{3/2}\log n)\right)$ time and that both counting algorithms allow us to output $x$ of those partial-cadences in $\mathcal{O}(xn)$ time.

As a special case, these results also hold for 3-cadences.

We further conclude from these results that the existence of $k$-cadences with at most $k-3$ errors as defined in Definition 5 can be detected in $\mathcal{O}\left(\min(|\Sigma|k^3n(\log n)^2, k^3n^{3/2}\log n)\right)$ time.

Without loss of generality, we will only deal with the case $a < b$ in this section.

▶ **Lemma 14.** *Three positions $x$, $y$ and $z$ form a $(a, b, c)$-partial-$k$-cadence if and only if*

- *the equation $\frac{y-x}{b-a} = \frac{z-y}{c-b} \in \mathbb{Z}$ holds,*
- *the equation $S[x] = S[y] = S[z]$ holds and*
- *the inequalities*

$$0 \geq \frac{(b+1)x - (a+1)y}{b-a}, \tag{1}$$

$$0 < \frac{bx - ay}{b-a}, \tag{2}$$

$$n \geq \frac{(b-k+1)x - (a-k+1)y}{b-a} \text{ and} \tag{3}$$

$$n < i + kd = \frac{(b-k)x - (a-k)y}{b-a} \text{ hold.} \tag{4}$$

**Proof.** Define $d := \frac{y-x}{b-a}$ and $i := x - ad$. Then $x = i + ad$ and $y = i + bd$. Furthermore, the equation $\frac{y-x}{b-a} = \frac{z-y}{c-b}$ holds if and only if $z = i + cd$ and $\frac{y-x}{b-a} \in \mathbb{Z}$ holds if and only if $d$ is an integer.

Additionally, using $x = i + ad$ and $y = i + bd$, the four inequalities can be simplified to $0 \geq i - d$, $0 < i$, $n \geq i + (k-1)d$ and $n < i + kd$.

Therefore, the lemma follows from the definition of the partial-cadence. ◀

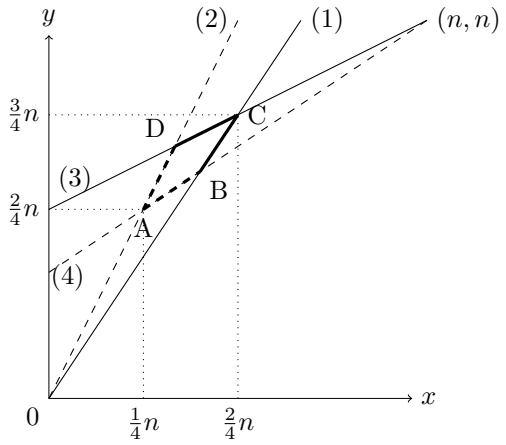


**Figure 5** The four inequalities of Lemma 14 for $(1, 2, 3)$-partial-4-cadences.

The four inequalities hold if the points $(x, y)$ lie inside the convex quadrilateral given, as shown in Figure 5, by the corners

$$A = \left(\frac{an}{k}, \frac{bn}{k}\right)$$
$$B = \left(\frac{(a+1)n}{k+1}, \frac{(b+1)n}{k+1}\right)$$
$$C = \left(\frac{(a+1)n}{k}, \frac{(b+1)n}{k}\right)$$
$$D = \left(\frac{an}{k-1}, \frac{bn}{k-1}\right)$$

including the vertex $C$ and the edges between $B$ and $C$ as well as between $C$ and $D$ but excluding all other vertices and the edges between $A$ and $B$ as well as between $D$ and $A$.

For given $x = i + ad$ and $y = i + bd$, the third occurrence $z = i + cd$ can be calculated with the equation $i + cd = \frac{(b-c)(i+ad)+(c-a)(i+bd)}{b-a}$ directly without calculating $i$ and $d$ first. The corresponding partial sums

$$c_k = \sum_{\substack{i+j=k \\ (i,j)\in P\cap\mathbb{Z}^2}} a_{\frac{i}{(b-c)}} b_{\frac{j}{(c-a)}}$$

can be calculated by using the partial sums

$$c_k = \sum_{\substack{i+j=k \\ (i,j)\in P'\cap\mathbb{Z}^2}} a'_i b'_j$$

with $a'_i := \begin{cases} a_{\frac{i}{b-c}} & \text{if } i \equiv 0 \pmod{b-c} \\ 0 & \text{otherwise} \end{cases}$ and $b'_j := \begin{cases} b_{\frac{j}{c-a}} & \text{if } j \equiv 0 \pmod{c-a} \\ 0 & \text{otherwise} \end{cases}$ and a polygon $P'$, which is derived from $P$ by stretching the first coordinate by $(b-c)$ and the second coordinate by $(c-a)$. The perimeter of $P'$ is at most $\max(|b-c|, |c-a|)$ times the perimeter of $P$. Using the quadrilateral $P = ABCD$ with perimeter

$$p \le 2|C_x - A_x| + 2|C_y - A_y| = 2\left(\frac{(a+1)n}{k} - \frac{an}{k}\right) + 2\left(\frac{(b+1)n}{k} - \frac{bn}{k}\right) = \frac{4n}{k} \in \mathcal{O}\left(\frac{n}{k}\right),$$

the polygon $P'$ has perimeter $p' \in \mathcal{O}(n)$. This proves the following three theorems.

▶ **Theorem 15.** *For every character $\sigma \in \Sigma$, the $(a, b, c)$-partial-$k$-cadences with $\sigma$ can be counted in $\mathcal{O}(n(\log n)^2)$ time. Also, if all $n_\sigma$ occurrences of $\sigma$ are known, the $(a, b, c)$-partial-$k$-cadences with $\sigma$ can be counted in $\mathcal{O}(n_\sigma^2)$ time.*

▶ **Theorem 16.** *The number of all $(a, b, c)$-partial-$k$-cadences can be counted in*

$$\mathcal{O}\left(\min(|\Sigma|n(\log n)^2, n^{3/2}\log n)\right) \text{ time.}$$

▶ **Theorem 17.** *After counting at least $x$ $(a, b, c)$-partial-$k$-cadences, it is possible to output $x$ $(a, b, c)$-partial-$k$-cadences in $\mathcal{O}(xn)$ time.*

Since every 3-cadence is an $(0, 1, 2)$-partial-3-cadence, we also obtain the special case:

▶ **Corollary 18.** *For every character $\sigma \in \Sigma$, the 3-cadences with $\sigma$ can be counted in $\mathcal{O}(n(\log n)^2)$ time. Also, if all $n_\sigma$ occurrences of $\sigma$ are known, the 3-cadences with $\sigma$ can be counted in $\mathcal{O}(n_\sigma^2)$ time.*

*Therefore, the number of all 3-cadences can be counted in*

$$\mathcal{O}\left(\min(|\Sigma|n(\log n)^2, n^{3/2}\log n)\right) \text{ time.}$$

*Also, after counting at least $x$ 3-cadences, it is possible to output $x$ 3-cadences in $\mathcal{O}(xn)$ time.*

Taking the sum over all possible triples $(a, b, c)$, we can also search for $k$-cadences with at most $k - 3$ errors. It can be checked in

$$\mathcal{O}\left(\min(|\Sigma|k^3n(\log n)^2, k^3n^{3/2}\log n)\right)$$

time whether the given string has a $k$-cadence with at most $k - 3$ errors. However, since $k$-cadences with less than $k - 3$ errors are counted more than once, it seems to be difficult to determine the exact number of $k$-cadences with at most $k - 3$ errors.

## 6 Conclusion

This paper extends convolutions to arbitrary convex polygons. One might wonder whether these convolutions could be sped up or be further extended to non-convex polynomials.

Instead of just partitioning the interior of the polygon into triangles, it is also possible to identify polygons by the difference of a slightly bigger but less complex polygon and a triangle. However, if the algorithm presented in this paper is adapted to non-convex polygons, it can generate self-intersecting polygons. While the time-complexity stays the same for these polygons, it becomes hard to ensure that every vertex and every edge of the polygon is counted exactly once.

Another approach is given by Levcopoulos and Lingas in [13]. This paper shows that any simple polygon can be decomposed into convex components in $\mathcal{O}(k \log k)$ time while only increasing the total perimeter by the factor $\mathcal{O}(\log k)$. This paper also shows that if the input polygon is rectilinear, this partition only contains axis-aligned rectangles. Since the convolution handles rectangles quicker and more easily than triangles, this saves a logarithm. However, in general, it is not obvious how to transform arbitrary polygons into equivalent simple rectilinear polygons in quasilinear time without blowing-up the number of vertices too much.

The non-rectangular convolution, unlike the usual convolution, allows us to define a dependence between the indices of the convoluted sequences. This dependence is not usable in applications like the multiplication of polynomials, and for many signal processing applications

this extended method does not seem to bring any benefits either. However, in order to count the partial-cadences this dependence was essential. The non-rectangular convolution may also have future applications in image processing and convolutional neural networks.

In terms of cadences, this paper presents algorithms to count and find sub-cadences, cadences and partial-cadences with three elements. However, if there are linearly many $c$-positions of $(a, b, c)$-partial-$k$-cadences, the knowledge of those partial-cadences does not lead to a sub-quadratic-time-algorithm for determining the existence 4-cadences. On the other hand, it is also not shown that this problem needs quadratic time.

Also, the time-complexity $\mathcal{O}(xn)$ for finding $x$ 3-cadences is quite pessimistic. If there are many 3-cadences, it is very likely that quite a few of these 3-cadences share one of their occurrences. These occurrences can be found in $\mathcal{O}(n)$ time. On the other hand, in the string $10^{n-1}1^{2n}$, for example, there are linearly many 3-cadences but every second occurrence and every third occurrence only occurs in at most one of those 3-cadences.

## References


1 R. C. Agarwal and C. S. Burrus. Number theoretic transforms to implement fast digital convolution. *Proceedings of the IEEE*, 63(4):550–560, April 1975. doi:10.1109/PROC.1975.9791.

2 Amihood Amir, Alberto Apostolico, Travis Gagie, and Gad M. Landau. String cadences. *Theoretical Computer Science*, 698:4–8, 2017. Algorithms, Strings and Theoretical Approaches in the Big Data Era (In Honor of the 60th Birthday of Professor Raffaele Giancarlo). doi:10.1016/j.tcs.2017.04.019.

3 N. C. Ankeny. The Least Quadratic Non Residue. *Annals of Mathematics*, 55(1):65–72, 1952. URL: http://www.jstor.org/stable/1969420.

4 Eric Bach and Jonathan Sorenson. Explicit bounds for primes in residue classes. *Math. Comput.*, 65(216):1717–1735, October 1996. doi:10.1090/S0025-5718-96-00763-6.

5 Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, 3rd Edition*. MIT Press, 2009. URL: http://mitpress.mit.edu/books/introduction-algorithms.

6 Svyatoslav Covanov and Emmanuel Thomé. Fast integer multiplication using generalized fermat primes. *Math. Comp.*, 88(317):1449–1477, 2019. doi:10.1090/mcom/3367.

7 Anindya. De, Piyush P. Kurur, Chandan. Saha, and Ramprasad. Saptharishi. Fast integer multiplication using modular arithmetic. *SIAM Journal on Computing*, 42(2):685–699, 2013. doi:10.1137/100811167.

8 J. Gardelle. Cadences. *Mathématiques et Sciences humaines*, 9:31–38, 1964. URL: http://www.numdam.org/item/MSH_1964__9__31_0.

9 D. Harvey and J. van der Hoeven. Faster integer multiplication using plain vanilla FFT primes. *Math. Comp.*, 88(315):501–514, 2019.

10 D. Harvey and J. van der Hoeven. Integer multiplication in time O(n log n). working paper or preprint, March 2019. URL: https://hal.archives-ouvertes.fr/hal-02070778.

11 D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. *Journal of Complexity*, 36:1–30, 2016. doi:10.1016/j.jco.2016.03.001.

12 D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Mathematical Proceedings of the Cambridge Philosophical Society*, 83(3):357–375, 1978. doi:10.1017/S0305004100054657.

13 Christos Levcopoulos and Andrzej Lingas. Bounds on the length of convex partitions of polygons. In Mathai Joseph and Rudrapatna Shyamasundar, editors, *Foundations of Software Technology and Theoretical Computer Science*, pages 279–295, Berlin, Heidelberg, 1984. Springer Berlin Heidelberg.

14 U. V. Linnik. On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):139–178, 1944.

**15** M. Lothaire. *Combinatorics on Words*. Cambridge Mathematical Library. Cambridge University Press, 1997. URL: `https://books.google.de/books?id=eATLTZzwW-sC`.

**16** Franz Mertens. Ein Beitrag zur analytischen Zahlentheorie. *Journal für die reine und angewandte Mathematik*, 78:46–62, 1874. URL: `http://eudml.org/doc/148244`.

**17** A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7(3):281–292, September 1971. `doi:10.1007/BF02242355`.

**18** William B. Thompson, Peter Shirley, and James A. Ferwerda. A Spatial Post-Processing Algorithm for Images of Night Scenes. *Journal of Graphics Tools*, 7(1):1–12, 2002. `doi:10.1080/10867651.2002.10487550`.

**19** Bartel Leendert van der Waerden. Beweis einer Baudet'schen Vermutung. *Nieuw Archief voor Wiskunde*, 15:212–216, 1927.

**20** Samuel S. Wagstaff. Greatest of the least primes in arithmetic progressions having a given modulus. *Mathematics of Computation*, 33(147):1073–1080, 1979. URL: `http://www.jstor.org/stable/2006082`.

**21** Triantafyllos Xylouris. *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, volume 404 of *Bonner Mathematische Schriften [Bonn Mathematical Publications]*. Universität Bonn, Mathematisches Institut, Bonn, 2011. Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.


## A Convolutions

It is well-known that the discrete acyclic convolution can be calculated with $\mathcal{O}(n \log n)$ complex arithmetic operations. However, if the convolution is calculated with the fast Fourier transform, the finite register lengths introduce roundoff errors. These errors can propagate and accumulate throughout the calculation.

Therefore, in order to calculate the convolution of integer sequences, it seems more convenient to use the number theoretic transform, which is the generalization of the fast Fourier transform from the field of the complex numbers to certain residue class rings.

In this section, we will show that after some precomputation in $\mathcal{O}\left(n(\log n)^2(\log\log n)\right)$ time it is possible to calculate these convolutions in $\mathcal{O}(n \log n)$ time.

Agarwal and Burrus show in [1] that the circular convolution of two integer vectors of length $n$ can be efficiently computed modulo a prime $p$ if $p-1$ is a multiple of $n$. Therefore we want to find a prime $p$ in the infinite arithmetic progression $\{n+1, 2n+1, 3n+1, \dots\}$.

The prime number theorem states that the number $\pi(N)$ of primes smaller than $N$ asymptotically behaves like $\frac{N}{\log N}$. Furthermore, Dirichlet's prime number theorem states that for a given $n$ and a sufficiently large $N$, the prime numbers are evenly distributed in all residue classes $mn + r$ with $\gcd(n, r) = 1$.

Therefore, for a given $n$ and sufficiently large $N$, we should expect circa $\frac{N}{\varphi(n) \log N}$ prime numbers of the form $mn + 1$ that are smaller than $N$. However, the "sufficient largeness" of $N$ depends on $n$. Therefore, these theorems do not provide the number of suitable primes smaller than the given number $N$.

Since the primes are expected to behave similarly in all coprime residue classes, Heath-Brown suggests in [12] that the least prime of the form $mn + 1$ is in $\mathcal{O}\left(n(\log n)^2\right)$. Wagstaff gives in [20] a heuristic argument to this conjecture and provides numerical evidence. However, the best proven upper bounds are much larger, even if the generalized Riemann hypothesis is assumed.

Linnik proves in [14] that there are constants $c$ and $L$ such that for each $n$, $r$ with $\gcd(n, r) = 1$, there is a prime of the form $mn + r$ with $mn + r < cn^L$. While Linnik himself did not provide the values of $c$ and $L$, there are some upper bounds: For example,

Xylouris proves in [21] (written in German) that there is a $c$ such that for each $n$, $r$ with $\gcd(n,r)=1$, there is a prime of the form $mn+r$ with $mn+r<cn^5$. More explicitly, Bach and Sorenson present in [4] that if the generalized Riemann hypothesis holds, for each $n$, $r$ with $\gcd(n,r)=1$, there is a prime of the form $mn+r$ with $mn+r<2(n\log n)^2$.

Without a shortcut allowing us to check the existence of a prime in a given finite arithmetic progression quickly, we have to test for each single number in this progression whether it is prime.

Therefore, using only the generalized Riemann hypothesis, we cannot expect to find a prime deterministically in $o\left(\frac{(n\log n)^2}{n}\right) = o\left(n(\log n)^2\right)$, even if we use on average only a constant time for each possible prime number.

Since this is already too slow for fast multiplications, numerous ways to solve or circumvent this problem have been established:

- Harvey and van der Hoeven propose in [10] a multiplication algorithm which uses $\mathcal{O}(n\log n)$ time by using the fast Fourier transform based on complex numbers.
- Some algorithms use stronger assumptions for the distribution of prime numbers. For example, Harvey and van der Hoeven use in [11] an unproven lower bound for the number of Mersenne primes and in [9] they assume that the least prime of the form $mn+c$ is in all coprime residue classes in $\mathcal{O}\left(\varphi(n)(\log n)^2\right)$. Also, Covanov and Thomé use in [6] an unproven lower bound for the number of generalized Fermat primes.
- Many algorithms do not use convolution of length $n$ but divide the number into blocks first and then use shorter convolutions over large rings. For example De et al. use the ring $\mathbb{Z}[\alpha]/\left(p^c,\alpha^m+1\right)$ in [7].
- While De et al. do not use it in their multiplication algorithm, they provide in [7] a randomized algorithm to find a suitable prime in expected running time $\widetilde{\mathcal{O}}((\log n)^3)$.

In the next theorem, we will show that the sieve of Eratosthenes comes close to the theoretical minimum of $\mathcal{O}\left(n(\log n)^2\right)$ for finding all primes of the form $mn+1$ up to $(n\log n)^2$.

The lengths of these primes is at most 4 times the length of $n$. Therefore, such a prime number $p_n$ is a good modulus for the convolution of length $n$ or any of its divisors.

▶ **Theorem 19.** *Let $n$ be an integer. A prime $p_n \equiv 1 \pmod{n}$ with $p_n < 2(n\log n)^2$ can be found in $\mathcal{O}(n(\log n)^2\log\log(n))$ time.*

**Proof.** The main idea is to use the sieve of Eratosthenes to first find all primes up to $2n\log n$ and then sieve only the numbers up to $2(n\log n)^2$ that are congruent to 1 modulo $n$ with these primes.

On the one hand, since $(2n\log n)^2 > 2(n\log n)^2$ holds, all numbers left after the second sieving are primes. On the other hand, the result of Bach and Sorenson in [4] guarantees that if the generalized Riemann hypothesis holds, there is a prime left. Also, by construction, all primes $p_n$ left fulfill this theorem.

It remains to be shown that this algorithm can be done in $\mathcal{O}(n(\log n)^2\log\log(n))$ time.

For the usual sieve of Eratosthenes, one prepares a Boolean array for the first $2n\log n$ numbers. Then, for each number that has not been marked as non-prime, every multiple is marked as non-prime. Afterwards, all non-marked numbers are returned. The majority of the time is spent for the marking. This takes

$$\mathcal{O}\left(\sum_{\substack{p=2\\ p \text{ is prime}}}^{2n\log n} \frac{2n\log n}{p}\right) = \mathcal{O}\left(n\log n \sum_{\substack{p=2\\ p \text{ is prime}}}^{2n\log n} \frac{1}{p}\right) = \mathcal{O}\left(n(\log n)(\log\log n)\right)$$

time. The last equality is given by Mertens in [16, p. 46] (written in German) and the inequality $\log\log(2n\log n) < 2\log\log(n)$.

For the second part, we have a much larger interval of numbers. However, since we only have to consider the first residue class, only every $n$-th number has to be considered. Therefore we need

$$\mathcal{O}\left(\sum_{\substack{p=2\\ p \text{ is prime}}}^{2n\log n} \frac{2(n\log n)^2}{np}\right) = \mathcal{O}\left(n(\log n)^2 \sum_{\substack{p=2\\ p \text{ is prime}}}^{2n\log n} \frac{1}{p}\right) = \mathcal{O}\left(n(\log n)^2(\log\log n)\right)$$

markings. Using the extended Euclidean algorithm, for every prime $p$, we can find the smallest $f$ such that $fp \equiv 1 \pmod{n}$ in $\mathcal{O}(\log p) \subseteq \mathcal{O}(\log n)$ time. Summing up over all primes, this takes

$$\mathcal{O}\left(\sum_{\substack{p=2\\ p \text{ is prime}}}^{2n\log n} \log n\right) \subseteq \mathcal{O}\left(n(\log n)^2\right)$$

time.

This concludes the proof. ◀

It is not only possible to find a suitable modulus for the number theoretic transform, but we can also find a suitable $2^t$-th root in the corresponding residue ring:

▶ **Theorem 20.** *Let $p_{2^t}$ be a prime with $p_{2^t} \equiv 1 \pmod{2^t}$ and $p_{2^t} < 2(2^t\log(2^t))^2$. A $2^t$-th root of unity modulo $p_{2^t}$ can be found in $\mathcal{O}\left((\log p_{2^t})^3\right)$ time.*

**Proof.** Let $p_{2^t} = 1 + o2^r$ for an odd number $o$.

Firstly, we will show that a residue $q^o$ is a $2^r$-th root of unity modulo $p_{2^t}$ if and only if $q$ is a quadratic nonresidue modulo $p_{2^t}$.

Since $p_{2^t}$ is prime, there is a primitive root $a$ modulo $p_{2^t}$.

Let $q \equiv a^i$. Then $q^o = a^{io}$ has the order $\frac{o2^r}{\gcd(io, o2^r)} = \frac{2^r}{\gcd(i, 2^r)}$. Therefore, $q^o$ has order $2^r$ if and only if $i$ is odd. On the other hand, if $i$ is even, then $q$ is a quadratic residue, and if $i$ is odd, then $q \equiv a^i = a\left(a^{\frac{i-1}{2}}\right)^2$ is a quadratic nonresidue. This implies that $q^o$ is a $2^r$-th root of unity modulo $p_{2^t}$ if and only if $q$ is a quadratic nonresidue modulo $p_{2^t}$.

Ankeny shows in [3] that if the generalized Riemann hypothesis holds, there is a quadratic nonresidue in the first $\mathcal{O}\left((\log p_{2^t})^2\right)$ residue classes. For any residue $q$ it can be tested with $\mathcal{O}(\log p_{2^t})$ multiplications and modulo operations whether $q^o$ has order $2^r$. As byproduct we get $(q^o)^{\left(2^{r-t}\right)}$. If and only if $q^o$ has order $2^r$, the power $(q^o)^{\left(2^{r-t}\right)}$ has order $2^t$.

Therefore, a $2^t$-th root of unity modulo $p_{2^t}$ can be found in $\mathcal{O}\left((\log p_{2^t})^3\right)$ time. ◀

Therefore, we can efficiently compute the integer convolution with the help of the number theoretic transform.

▶ **Theorem 21.** *For a given integer $N$, we can find a modulus $p_N$ and a suitable root $q_N$ in $\mathcal{O}\left(N(\log N)^2(\log\log N)\right)$ time such that it is possible to calculate the acyclic convolution modulo $p_N$ of two sequences of length $n \leq N$ in $\mathcal{O}(n\log n)$ time afterwards.*

**Proof.** The acyclic convolution of sequences of length $n$ can be derived from a circular convolution of sequences with lengths of at least $2n$. Therefore, we will first prepare circular convolutions of length $2^T$ with $2N \leq 2^T < 4N$.

For this length, the last two theorems state that a suitable modulus $p_N$ and a suitable $2^T$-th root $q_N$ of unity can be found in $\mathcal{O}\left(N(\log N)^2(\log\log N)\right)$.

Afterwards, for every $n \leq N$ we can append zeros to get the length $2^t$ with $2n \leq 2^t < 4n$. Since $2^t$ is a divisor of $2^T$, we can use $(q_N)^{\left(2^{T-t}\right)}$ as $2^t$-th root of unity.

This allows the calculation of the acyclic convolution modulo $p_N$ in $\mathcal{O}\left(n \log n\right)$ time. ◀