COARSE-GRAINED INTEGERS

Smooth? Rough? Both!

Daniel Loebenberger and Michael Nüsken

November 9, 2012

Abstract. We count $]B, C]$-grained, k-factor integers which are simultaneously B-rough and C-smooth and have a fixed number k of prime factors. Our aim is to exploit explicit versions of the prime number theorem as much as possible to get good explicit bounds for the count of such integers. This analysis was inspired by certain inner procedures in the general number field sieve. The result should at least provide some insight in what happens there.

We estimate the given count in terms of some recursively defined functions. Since they are still difficult to handle, only another approximation step reveals their orders.

Finally, we use the obtained bounds to perform numerical experiments that show how good the desired count can be approximated for the parameters of the general number field sieve in the mentioned inspiring application.

Keywords. Smooth numbers, rough numbers, counting, prime number theorem, general number field sieve, RSA.

Subject classification. 11Axx,11N05,11N25

Let us call an integer *$\mathcal{A}$-grained* iff all its prime factors are in the set $\mathcal{A}$. Then an integer is *C-smooth* iff it is $]0, C]$-grained, and *B-rough* iff it is $]B, \infty[$-grained. You may want to call an integer family *coarse-grained* if it is $]B, C]$-grained and the number of factors is bounded. We consider the number of integers up to a real positive bound x that are $]B, C]$-grained and have a given number k of factors, in formulae:

$$\pi^k_{B,C}(x) := \# \left\{ n \leq x \,\middle|\, \exists p_1, \ldots, p_k \in \mathbb{P} \cap \,]B, C] \colon n = p_1 \cdots p_k \right\}. \tag{0.1}$$

We always assume that $C > B$, since otherwise the set under consideration is empty.

Such numbers occur for example in an intermediate step in the number field sieve when trying to factor large numbers. During the sieving integers are constructed as random values of carefully chosen small-degree polynomials and made B-rough by dividing out all smaller factors. The remaining number is fed into an elliptic curve factoring algorithm with a time limit that should allow to find factors up to C. To tune the overall algorithm it is vital to know the probability that the remaining number is C-smooth. Assuming that the polynomials output true random numbers the counting task we deal with is the missing link since estimates for counting B-smooth numbers are known, see for example the overview by Granville (2008). It is difficult, however, to compare our results to existing ones, since we consider integers with a *fixed* number of factors. This restriction is completely sufficient for the application we have in mind. To our knowledge these kind of investigations cannot be found in the literature. Our main result implies the following

COROLLARY. *Fix $k \in \mathbb{N}_{\geq 2}$, $\alpha > 0$ and $\varepsilon > 0$. Then for large B and $C = B^{1+\alpha}$ we have uniformly for $x \in [B^k(1+\varepsilon), C^k(1-\varepsilon)]$ that*

$$\pi^k_{B,C}(x) \in \Theta\left(\frac{x}{\ln B}\right). \qquad \square$$

Actually, we can describe a piecewise smooth function that approximates $\pi^k_{B,C}$ up to an additive error of order $\mathcal{O}\left(\frac{x}{\sqrt{B}}\right)$ and the hidden constant depends on ε, k and α only, see Theorem 9.2, Theorem 9.3.

To avoid difficulties with non-squarefree numbers, instead of numbers we count lists of primes

$$\text{(0.2)} \qquad \kappa^k_{B,C}(x) := \#\left\{(p_1,\ldots,p_k) \in (\mathbb{P} \cap \,]B,C])^k \,\middle|\, p_1 \cdots p_k \leq x\right\}.$$

It turns out that there are anyways only a few non-squarefree numbers counted by $\pi^k_{B,C}$, namely $k! \cdot \pi^k_{B,C}(x) \approx \kappa^k_{B,C}(x)$. This would actually be an equality if there were no non-squarefree numbers in the count. We defer a precise treatment until Section 8.

We head for determining precise bounds $\kappa^k_{B,C}(x)$ or $\pi^k_{B,C}(x)$ that can be used in practical situations. However, to understand these bounds we additionally consider the asymptotical behaviours. This is tricky since we have to deal with the three parameters B, C and x simultaneously. To guide us in considering different asymptotics, we usually write $B = x^\beta$, $C = x^\gamma$ and $\gamma = \beta(1+\alpha)$. In particular, $C = B^{1+\alpha}$. So we replace (B, C, x) with (x, β, γ) or (x, α, β), similar to the considerations when counting smooth or rough numbers in the literature. Alternatively, it seems also natural to fix x somehow in the interval $]B^k, C^k]$ by introducing a parameter ξ by

$$x = B^{k-\xi}C^\xi = B^{k+\xi\alpha}.$$

Now the parameters are (B, C, ξ) or (B, α, ξ).

As a first observation, note that $\kappa^k_{B,C}(x)$ is constantly 0 for $x < B^k$ and constantly $(\pi(C) - \pi(B))^k$ for $x \geq C^k$ and grows monotonically when x goes through $[B^k, C^k]$. Here π denotes the prime counting function. For 'middle' x-values the asymptotics can be derived from our main result:

COROLLARY. *Fix $k \in \mathbb{N}_{\geq 2}$, $\alpha > 0$ and $\varepsilon > 0$. Then for large B and $C = B^{1+\alpha}$ we have uniformly for $x \in [B^k(1+\varepsilon), C^k(1-\varepsilon)]$ that*

$$\kappa^k_{B,C}(x) \in \Theta\left(\frac{x}{\ln B}\right) = \Theta\left(\frac{x}{\beta \ln x}\right).$$

Later, we specify a piecewise smooth function $\widetilde{\kappa}^k_{B,C}$ which approximates $\kappa^k_{B,C}$ with an error of order $\mathcal{O}\left(\frac{x}{\sqrt{B}}\right)$ where the hidden constants depend on ε, k and α only, see Theorem 3.2, Theorem 3.5, and subsequent considerations.

The preceeding result is in contrast to the asymptotics at $x = C^k$:

$$\kappa^k_{B,C}\left(C^k\right) \approx \frac{C^k}{\ln^k C} = \frac{B^{k(1+\alpha)}}{(1+\alpha)^k \ln^k B} \in \Theta\left(\frac{x}{\beta^k \ln^k x}\right).$$

This observation is explained as follows: Note that roughly half of the numbers up to x are in the interval $[\frac{1}{2}x, x]$ and similarly for primes. Thus the behaviour of those candidates largely rule $\kappa^k_{B,C}(x)/x$. For an $x = B^{k-\xi}C^{\xi}$ with a fixed $\xi \in \left]0, k\right[$, it is mostly determined by the requirement that the counted numbers are B-rough, and we thus observe a comparatively large fraction of $\left]B, C\right]$-grained numbers. In the extreme case $x = C^k$, most candidates are ruled out by the requirement to be C-smooth and thus we see a much smaller fraction of $\left]B, C\right]$-grained numbers.

The case that the intervals $\left]B^k, C^k\right]$ are disjoint for considered values k is especially nice, as then the number of prime factors of a B-smooth and C-rough number n can be derived from the number n. So we assume in the entire paper that $C < B^s$ for some fixed $s > 1$. (Clearly, we cannot have a fixed s that grants disjointness for all intervals. But for the first few we can.) In the inspiring number field sieve application we have $C < B^{1.232⊤}$.[1] This ensures that the intervals $\left]B^k, C^k\right]$ for $k \leq 5$ are disjoint.

A further application is related to RSA. Decker & Moree (2008) give estimates for the number of RSA-integers. They use one ad-hoc definition proposed by B. de Weger. However, it is not so clear which numbers we should call RSA-integers. A discussion and further calculations to adapt our results to the different shape are needed. We have treated these issues in Loebenberger & Nüsken (2011).

As our basic field of interest is cryptography and there the largest occurring numbers are actually small in the number theorist's view, we assume the Riemann hypothesis throughout the entire paper. We use the following version of the prime number theorem:

Prime number theorem 0.3 (Von Koch 1901, Schoenfeld 1976). *If (and only if) the Riemann hypothesis holds then for $x \geq 2657$*

$$|\pi(x) - \mathrm{li}(x)| < \frac{1}{8\pi}\sqrt{x}\ln x,$$

where $\mathrm{li}(x) = \int_0^x \frac{1}{\ln t}\,\mathrm{d}t$.

[1] Side remark: to indicate how a real number was rounded we append a special symbol. Examples: π = 3.14⊥ = 3.142Ұ = 3.1416⊤ = 3.14159⊥. The height of the platform shows the size of the left-out part and the direction of the antenna indicates whether actual value is larger or smaller than displayed. We write, say, e = 2.72⊤ = 2.71⊓ as if the shorthand were exact.

We have numerically verified this inequality for $x \leq 2^{40} \approx 1.1 \cdot 10^{12}$ based on Kulsha's tables (Kulsha 2008) and extensions built using the segmented siever implemented by Oliveira e Silva (2003). We are confident that we can extend this verification much further. In the inspiring application we have $x < 2^{37}$ and so for those x we can take this theorem for granted even if the Riemann hypothesis should not hold.

We arrive at the following description of the desired count:

THEOREM. *Let* $B < C = B^{1+\alpha}$ *with* $\alpha \geq \frac{\ln B}{\sqrt{B}}$ *and fix* $k \geq 2$*. Then for any (small)* $\varepsilon > 0$ *and* B *tending to infinity we have for* $x \in \left[B^k(1+\varepsilon), C^k(1-\varepsilon)\right]$ *a value* $\widetilde{a} \in \left[\frac{\alpha^{k-1}\breve{c}_k}{k!(1+\alpha)^k}, \frac{1}{k!}\right]$ *with* $\breve{c}_k = \min\left(2^{-4}\frac{\varepsilon^k}{k!}, 2^{-k}\frac{\varepsilon^{k-1}}{(k-1)!}\right)$ *such that*

$$\left|\pi^k_{B,C}(x) - \widetilde{a}\frac{x}{\ln B}\right| \leq (2^k - 1)\alpha^{k-2}(1+\alpha) \cdot \frac{x}{\sqrt{B}} + 2^{k-1}\frac{x}{B}. \qquad \square$$

Also without assuming the Riemann hypothesis we can achieve meaningful results provided we use a good unconditional version of the prime number theorem whose error estimate is at least in $\mathcal{O}\left(\frac{x}{\ln^3 x}\right)$. The famous work by Rosser & Schoenfeld (1962, 1975) is not sufficient. Yet, Dusart (1998) provides an explicit error bound of order $\mathcal{O}\left(\frac{x}{\ln^3 x}\right)$, and Ford (2002a) provides explicit error bounds of order $\mathcal{O}\left(x \exp\left(-\frac{A(\ln x)^{3/5}}{(\ln \ln x)^{1/5}}\right)\right)$ though this only applies for x beyond 10^{171} or even much later depending on A and the $\mathcal{O}$-constant, see Fact 6.1.

1. The recursion

The essential basis for the analysis of the counting functions $\kappa^k_{B,C}$ is the following simple description.

LEMMA 1.1. *For all* $k \in \mathbb{N}_{>0}$ *we have the recursion*

$$\kappa^k_{B,C}(x) = \sum_{p_k \in \mathbb{P} \cap]B,C]} \kappa^{k-1}_{B,C}(x/p_k)$$

based on

$$\kappa^0_{B,C}(x) = \begin{cases} 0 & \text{if } x \in [0,1[, \\ 1 & \text{if } x \in [1,\infty[. \end{cases}$$

PROOF. In case $k > 0$ we have

$$\begin{aligned} \kappa^k_{B,C}(x) &= \#\left\{(p_1,\ldots,p_k) \in (\mathbb{P} \cap]B,C])^k \;\middle|\; p_1 \cdots p_k \leq x\right\} \\ &= \# \biguplus_{p \in \mathbb{P} \cap]B,C]} \left\{(p_1,\ldots,p_k) \in (\mathbb{P} \cap]B,C])^k \;\middle|\; \begin{array}{r} p_1 \cdots p_{k-1} \leq x/p_k, \\ p_k = p \end{array}\right\} \\ &= \sum_{p_k \in \mathbb{P} \cap]B,C]} \kappa^{k-1}_{B,C}(x/p_k). \end{aligned}$$

The case $k = 0$ is immediate from the definition. □

From the definition (0.2) or from Lemma 1.1, it is clear that

$$\kappa^1_{B,C}(x) = \begin{cases} 0 & \text{if } x \in [0, B[, \\ \pi(x) - \pi(B) & \text{if } x \in [B, C[, \\ \pi(C) - \pi(B) & \text{if } x \in [C, \infty[. \end{cases}$$

This reveals that the case distinction in $\kappa^0_{B,C}$ leaves its traces on higher $\kappa^k_{B,C}$. For further calculations it is vital that we make this precise. This will enable us later to do our estimates. For $k \in \mathbb{N}$ we distinguish $k+2$ cases:

$$\begin{aligned} x \text{ is in case } (k,-1) &:\Longleftrightarrow x \in \Big[0, B^k\Big[, \\ x \text{ is in case } (k,j) &:\Longleftrightarrow x \in \Big[B^{k-j}C^j, B^{k-1-j}C^{j+1}\Big[, \\ x \text{ is in case } (k,k) &:\Longleftrightarrow x \in \Big[C^k, \infty\Big[, \end{aligned}$$

where $j \in \mathbb{N}_{<k}$. Note that most cases are characterized by the exponent of C at the left end of the interval.

Lemma 1.2. *For $k, j \in \mathbb{N}$, $0 \le j < k$ and x in case (k,j), we have*

$$\kappa^k_{B,C}(x) = \sum_{p_k \in \mathbb{P} \cap \left]\frac{x}{B^{k-1-j}C^j}, C\right]} \kappa^{k-1}_{B,C}(x/p_k) + \sum_{p_k \in \mathbb{P} \cap \left]B, \frac{x}{B^{k-1-j}C^j}\right]} \kappa^{k-1}_{B,C}(x/p_k)$$

where in the first sum x/p_k is in case $(k-1, j-1)$ and in the second in case $(k-1, j)$. For $j = -1$, and $j = k$ we do not split the sum, as then all x/p_k are in one case anyways. For $j = 0$ the left part is zero, so that the splitting there is less visible.

Proof. We only have to verify that $x/p_k \in \big[B^{k-1-j}C^j, B^{k-j-2}C^{j+1}\big[$ for $p_k \in \mathbb{P} \cap]B, {}^{x}/_{B^{k-1-j}C^j}]$ and $x \in \big[B^{k-j}C^j, B^{k-1-j}C^{j+1}\big[$. Similarly, the statement for the second sum is established. □

For example, we obtain

$$\kappa^2_{B,C}(x) = \begin{cases} 0 & \text{if } x \in \big[0, B^2\big[, \\ \sum_{p_2 \in \mathbb{P} \cap \left]B, \frac{x}{B}\right]} \sum_{p_1 \in \mathbb{P} \cap \left]B, \frac{x}{p_2}\right]} 1 & \text{if } x \in \big[B^2, BC\big[, \\ \sum_{p_2 \in \mathbb{P} \cap \left]\frac{x}{C}, C\right]} \sum_{p_1 \in \mathbb{P} \cap \left]B, \frac{x}{p_2}\right]} 1 & \\ \quad + \sum_{p_2 \in \mathbb{P} \cap \left]B, \frac{x}{C}\right]} \sum_{p_1 \in \mathbb{P} \cap]B, C]} 1 & \text{if } x \in \big[BC, C^2\big[, \\ \sum_{p_2 \in \mathbb{P} \cap]B, C]} \sum_{p_1 \in \mathbb{P} \cap]B, C]} 1 & \text{if } x \in \big[C^2, \infty\big[. \end{cases} \tag{1.3}$$

So for $\kappa^2_{B,C}(x)$ we have four cases with four 2-fold sums. In general $\kappa^k_{B,C}(x)$ has $k+2$ cases with 2^k k-fold sums. Well, we better stop unfolding here.

Based on the intuition that a randomly selected integer n is prime with probability $\frac{1}{\ln n}$ we can replace $\sum_{p\in\mathbb{P}\cap]B,C]} f(p)$ with $\int_B^C \frac{f(p)}{\ln p}\,\mathrm{d}p$. This directly leads to the approximation function. We prefer however to follow a better founded way to them which will also give information about the error term.

2. Using estimates

From the recursion for $\kappa^k_{B,C}(x)$ it is clear that we have to compute terms like

$$\sum_{p\in\mathbb{P}\cap]B,C]} f(p) \quad \text{or} \quad \sum_{p\in\mathbb{P}\cap]B,C]} f(x/p).$$

To get good estimates for such a sum we follow the classic path, as Rosser & Schoenfeld (1962): we rewrite the sum as a Lebesque-Stieltjes-integral over the prime counting function $\pi(p)$. Then we substitute $\pi(t) = \mathrm{Li}(t) + E(t)$, keeping in mind that we know good bounds on the error term $E(t)$ by the Prime number theorem 0.3. Finally, we integrate by parts, estimate and integrate by parts back:

$$\begin{aligned}
&\sum_{p\in\mathbb{P}\cap]B,C]} f(p)\\
&= \int_B^C f(t)\,\mathrm{d}\pi(t)\\
&= \int_B^C f(t)\,\mathrm{d}\,\mathrm{Li}(t) + \int_B^C f(t)\,\mathrm{d}E(t)\\
&= \int_B^C \frac{f(t)}{\ln t}\,\mathrm{d}t + f(C)E(C) - f(B)E(B) - \int_B^C E(t)\,\mathrm{d}f(t)\,.
\end{aligned}$$

The existence of all integrals follow from the existence of the first. If the sum kernel f is differentiable with respect to t we can rewrite $\int_B^C E(t)\,\mathrm{d}f(t) = \int_B^C f'(t)E(t)\,\mathrm{d}t$. Now we can use the estimate on the error term $E(t)$:

$$\begin{aligned}
&\left|\sum_{p\in\mathbb{P}\cap]B,C]} f(p) - \int_B^C \frac{f(t)}{\ln t}\,\mathrm{d}t\right|\\
&\leq |f(C)|\widehat{E}(C) + |f(B)|\widehat{E}(B) + \int_B^C |f'(t)|\widehat{E}(t)\,\mathrm{d}t.
\end{aligned}$$

What remains is, given the concrete f, to determine the occurring integrals. For the counting functions $\kappa^k_{B,C}$ —as one would guess— this task is more and more complicated the larger k is. Clearly, smoothness properties of f must be considered carefully.

During all this we make sure that the involved functions stay sufficiently smooth:

Lemma 2.1 (Prime sum approximation). *Let f, $\widetilde{f}$, $\widehat{f}$ be functions $\mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}$ such that $\widetilde{f}$ and $\widehat{f}$ are piecewise continuous, $\widetilde{f} + \widehat{f}$ is increasing, and*

$$\left| f(x) - \widetilde{f}(x) \right| \leq \widehat{f}(x)$$

for $x \in \mathbb{R}_{>0}$. Further, let $\widehat{E}(p)$ be a positive valued, increasing, smooth function of p bounding $|\pi(p) - \mathrm{Li}(p)|$ on $[B, C]$. (For example, under the Riemann hypothesis we can take $\widehat{E}(p) = \frac{1}{8\pi}\sqrt{p}\ln p$ provided $p \geq 2657$.) Then for $x \in \mathbb{R}_{>0}$

$$\left| \sum_{p \in \mathbb{P} \cap]B,C]} f(x/p) - \quad \widetilde{g}(x) \quad \right| \leq \widehat{g}(x)$$

where

$$\begin{aligned}
\widetilde{g}(x) &= \int_B^C \frac{\widetilde{f}(x/p)}{\ln p} \,\mathrm{d}p\,, \\
\widehat{g}(x) &= \int_B^C \frac{\widehat{f}(x/p)}{\ln p} \,\mathrm{d}p + 2(\widetilde{f} + \widehat{f})(x/B)\widehat{E}(B) + \int_B^C \left(\widetilde{f} + \widehat{f}\right)(x/p)\widehat{E}'(p) \,\mathrm{d}p\,.
\end{aligned}$$

Moreover, $\widetilde{g}$ and $\widehat{g}$ are piecewise continuous, and $\widetilde{g} + \widehat{g}$ is increasing.

Proof. The assumption immediately implies

$$\left| \sum_{p \in \mathbb{P} \cap]B,C]} f(x/p) - \sum_{p \in \mathbb{P} \cap]B,C]} \widetilde{f}(x/p) \right| \leq \sum_{p \in \mathbb{P} \cap]B,C]} \widehat{f}(x/p).$$

Using the techniques just sketched we obtain $\sum_{p \in \mathbb{P} \cap]B,C]} \widetilde{f}(x/p) = \int_B^C \frac{\widetilde{f}(x/p)}{\ln p} \,\mathrm{d}p + \int_B^C \widetilde{f}(x/p) \,\mathrm{d}E(p)$ with $E(p) = \pi(p) - \mathrm{Li}(p)$. Shifting the second term to the correspondingly transformed error bound, we now have

$$\left| \sum_{p \in \mathbb{P} \cap]B,C]} f(x/p) - \underbrace{\int_B^C \frac{\widetilde{f}(x/p)}{\ln p} \,\mathrm{d}p}_{= \widetilde{g}(x)} \right| \leq \int_B^C \frac{\widehat{f}(x/p)}{\ln p} \,\mathrm{d}p + \int_B^C (\widehat{f} + \widetilde{f})(x/p) \,\mathrm{d}E(p)\,.$$

This bound always holds, yet we still have to estimate $E(p)$ in it. Abbreviating

$h(p) = (\widetilde{f} + \widehat{f})(x/p)$ we estimate the last integral:

$$\begin{aligned}\int_B^C h(p)\ \mathrm{d}E(p) &= h(C)E(C) - h(B)E(B) - \int_B^C E(p)\ \mathrm{d}h(p) \\ &\le h(C)\widehat{E}(C) + h(B)\widehat{E}(B) - \int_B^C \widehat{E}(p)\ \mathrm{d}h(p) \\ &= \ + h(C)\widehat{E}(C) + h(B)\widehat{E}(B) \\ &\quad - h(C)\widehat{E}(C) + h(B)\widehat{E}(B) \\ &\quad + \int_B^C h(p)\ \mathrm{d}\widehat{E}(p)\,.\end{aligned}$$

For the inequality we use that $h(p)$ is *decreasing* in p. Collecting gives the claim.

Finally, $\widetilde{g}$ and $\widehat{g}$ being obviously piecewise continuous it remains to show that $\widetilde{g} + \widehat{g}$ is increasing. By the (defining) equation

$$(\widetilde{g} + \widehat{g})(x) = \int_B^C (\widetilde{f} + \widehat{f})(x/p) \left(\frac{1}{\ln p} + \widehat{E}'(p)\right)\ \mathrm{d}p + 2(\widetilde{f} + \widehat{f})(x/B)\widehat{E}(B)$$

this follows from $\widetilde{f} + \widehat{f}$ and $\widehat{E}$ being increasing. □

3. Approximations

Based on Lemma 2.1 we recursively define approximation functions $\widetilde{\kappa}^k_{B,C}$ and error bounding functions $\widehat{\kappa}^k_{B,C}$. Recursive application of Lemma 2.1 will lead to a good estimate in Theorem 3.2. For the understanding we further need to determine the asymptotic order of the functions defined here, which we start in the remainder of this section. Theorem 3.5 relates the functions $\widetilde{\kappa}^k_{B,C}$ and $\widehat{\kappa}^k_{B,C}$ to some easier manageable functions. These in turn are computed or estimated, respectively, in Section 4 and Section 5.

Definition 3.1. *For $x \ge 0$ we define*

$$\widetilde{\kappa}^0_{B,C}(x) := \kappa^0_{B,C}(x)\,, \qquad \widehat{\kappa}^0_{B,C}(x) := 0$$

and recursively for $k > 0$

$$\begin{aligned}\widetilde{\kappa}^k_{B,C}(x) &:= \int_B^C \frac{\widetilde{\kappa}^{k-1}_{B,C}(x/p_k)}{\ln p_k}\ \mathrm{d}p_k\,, \\ \widehat{\kappa}^k_{B,C}(x) &:= \int_B^C \frac{\widehat{\kappa}^{k-1}_{B,C}(x/p_k)}{\ln p_k}\ \mathrm{d}p_k \\ &\quad + 2\left(\widetilde{\kappa}^{k-1}_{B,C} + \widehat{\kappa}^{k-1}_{B,C}\right)(x/B)\widehat{E}(B) \\ &\quad + \int_B^C \left(\widetilde{\kappa}^{k-1}_{B,C} + \widehat{\kappa}^{k-1}_{B,C}\right)(x/p_k)\widehat{E}'(p_k)\ \mathrm{d}p_k\,.\end{aligned}$$

These functions now describe the behavior of $\kappa^k_{B,C}$ nicely:

THEOREM 3.2. *Given $x \in \mathbb{R}_{>0}$ and $k \in \mathbb{N}$. Then the inequality*

$$\left|\kappa^k_{B,C}(x) - \widetilde{\kappa}^k_{B,C}(x)\right| \leq \widehat{\kappa}^k_{B,C}(x)$$

holds.

PROOF. Using Lemma 2.1 the claim together with the fact that $\widetilde{\kappa}^k_{B,C} + \widehat{\kappa}^k_{B,C}$ is increasing follow simultaneously by induction on k based on $\widetilde{\kappa}^0_{B,C} = \kappa^0_{B,C}$ and $\widehat{\kappa}^0_{B,C} = 0$. □

In order to give a first impression we calculate $\widetilde{\kappa}^1_{B,C}$ and $\widehat{\kappa}^1_{B,C}$. Analogous to Lemma 1.2, we split the integration at ${}^x/_{B^{k-1-j}C^j}$ so that the parts fall entirely into case $(k-1, j-1)$ or into case $(k-1, j)$:

$$\widetilde{\kappa}^k_{B,C}(x) = \int_{{}^x/_{B^{k-1-j}C^j}}^{C} \widetilde{\kappa}^{k-1}_{B,C}(x/p_k)\ \mathrm{d}p_k + \int_B^{{}^x/_{B^{k-1-j}C^j}} \widetilde{\kappa}^{k-1}_{B,C}(x/p_k)\ \mathrm{d}p_k\,.$$

Also for $\widehat{\kappa}^k_{B,C}$ this can be done, simply split the occurring integrals at ${}^x/_{B^{k-1-j}C^j}$. Now unfolding the recursive definition of $\widetilde{\kappa}^1_{B,C}$ gives:

$$\widetilde{\kappa}^1_{B,C}(x) = \begin{cases} 0 & \text{if } x \in [0, B[, \\ \int_B^x \frac{1}{\ln p_1}\ \mathrm{d}p_1 & \text{if } x \in [B, C[, \\ \int_B^C \frac{1}{\ln p_1}\ \mathrm{d}p_1 & \text{if } x \in [C, \infty[, \end{cases}$$

$$\widehat{\kappa}^1_{B,C}(x) = \begin{cases} 0 & \text{if } x \in [0, B[, \\ \widehat{E}(x) + \widehat{E}(B) & \text{if } x \in [B, C[, \\ \widehat{E}(C) + \widehat{E}(B) & \text{if } x \in [C, \infty[, \end{cases}$$

which corresponds exactly to the approximation of the prime counting function by the logarithmic integral Li. In case $k = 2$ we obtain

$$\widetilde{\kappa}^2_{B,C}(x) = \begin{cases} 0 & \text{if } x \in \left[0, B^2\right[, \\ \int_B^{\frac{x}{B}} \int_B^{\frac{x}{p_2}} \frac{1}{\ln p_1 \ln p_2}\ \mathrm{d}p_1\ \mathrm{d}p_2 & \text{if } x \in \left[B^2, BC\right[, \\ \int_{\frac{x}{C}}^C \int_B^{\frac{x}{p_2}} \frac{1}{\ln p_1 \ln p_2}\ \mathrm{d}p_1\ \mathrm{d}p_2 & \\ \quad + \int_B^{\frac{x}{C}} \int_B^C \frac{1}{\ln p_1 \ln p_2}\ \mathrm{d}p_1\ \mathrm{d}p_2 & \text{if } x \in \left[BC, C^2\right[, \\ \int_B^C \int_B^C \frac{1}{\ln p_1 \ln p_2}\ \mathrm{d}p_1\ \mathrm{d}p_2 & \text{if } x \in \left[C^2, \infty\right[. \end{cases} \tag{3.3}$$

This is now exactly the transformed version of (1.3), as announced there. You may ask where you can find a display of the error term corresponding to (3.3). Well, we have computed it. But the resulting terms are so complex that we didn't really learn much from it. Here is an expression for $x \in \left[B^2, BC\right[$:

$$\begin{aligned}\widehat{\kappa}^2_{B,C}(x) = &\int_B^{\frac{x}{B}} \int_B^{\frac{x}{p}} \left(\frac{\widehat{E}'(q)}{\ln p} + \frac{\widehat{E}'(p)}{\ln q} + \widehat{E}'(p)\widehat{E}'(q)\right) \,\mathrm{d}q\ \mathrm{d}p \\ &+ 4\widehat{E}(B)\int_B^{\frac{x}{B}} \frac{1}{\ln p}\,\mathrm{d}p + 4\widehat{E}(B)\widehat{E}(x/B)\end{aligned}$$

Though this term is still handleable, it becomes apparent that things get more and more complicated with increasing k. We escape from this issue by loosening the bonds and weakening our bounds slightly. The first aim will be to obtain easily computable terms while retaining the asymptotic orders, the second aim will be to still retain meaningful bounds for the fixed values $B = 1100 \cdot 10^6$, $C = 2^{37} - 1$, $k \in \{2, 3, 4\}$ from our inspiring application.

Our next task is to describe the orders of $\widetilde{\kappa}^k_{B,C}$ and $\widehat{\kappa}^k_{B,C}$. The main problem in an exact calculation is that most of the time we cannot elementary integrate a function with a logarithm occurring in the denominator. But using $B \leq p \leq C$ we can obtain a suitably good approximation instead by replacing $\frac{1}{\ln p}$ with $\frac{1}{\ln B}$ in the integrals. At this point we start using $C \leq B^s$ and rewrite $C = B^{1+\alpha}$ where α is a new parameter (bounded by $s-1$). For the time being you can consider α as a constant, but actually we make no assumption on it. This leads to the following

Definition 3.4. *For $x \geq 0$ we let*

$$\widetilde{\lambda}^0(x) := \kappa^0_{B,C}(x), \qquad \widehat{\lambda}^0(x) := 0,$$

and recursively for $k > 0$

$$\begin{aligned}\widetilde{\lambda}^k(x) &:= \int_B^C \frac{\widetilde{\lambda}^{k-1}(x/p_k)}{\ln B}\,\mathrm{d}p_k\,, \\ \widehat{\lambda}^k(x) &:= \int_B^C \frac{\widehat{\lambda}^{k-1}(x/p_k)}{\ln B}\,\mathrm{d}p_k \\ &\quad + 2\left(\widetilde{\lambda}^{k-1} + \widehat{\lambda}^{k-1}\right)(x/B)\,\widehat{E}(B) \\ &\quad + \int_B^C \left(\widetilde{\lambda}^{k-1} + \widehat{\lambda}^{k-1}\right)(x/p_k)\,\widehat{E}'(p_k)\,\mathrm{d}p_k\,.\end{aligned}$$

We observe that $\ln B \leq \ln p_k \leq \ln C = (1+\alpha)\ln B$. Thus we obtain $\int_B^C \frac{f(p)}{\ln p}\,\mathrm{d}p \in \left[\frac{1}{1+\alpha}, 1\right] \int_B^C \frac{f(p)}{\ln B}\,\mathrm{d}p$ for any positive integrable function f. By induction on k we obtain

Theorem 3.5. *Write $C = B^{1+\alpha}$ and fix $k \in \mathbb{N}_{>0}$. Then for $x \in \mathbb{R}_{>0}$ we have*

$$\widetilde{\kappa}^k_{B,C}(x) \in \left[\frac{1}{(1+\alpha)^k}, 1\right] \widetilde{\lambda}^k(x),$$
$$\widehat{\kappa}^k_{B,C}(x) \in \left[\frac{1}{(1+\alpha)^k}, 1\right] \widehat{\lambda}^k(x). \qquad \square$$

In order to determine at least the asymptotic orders of $\widetilde{\kappa}^k_{B,C}$ and $\widehat{\kappa}^k_{B,C}$ (along with precise estimates) it remains to solve the recursions for $\widetilde{\lambda}^k$ and $\widehat{\lambda}^k$, or at least to estimate these functions. As a first step, we rewrite all integrals in Definition 3.4 in terms of ϱ defined by $p_k = B^{1+\varrho\alpha}$.

Definition 3.4 continued. *Rewrite $x = B^{k+\xi\alpha}$ with a new parameter ξ and let $\widetilde{\lambda}^k\langle\xi\rangle := \widetilde{\lambda}^k\left(B^{k+\xi\alpha}\right)$ and $\widehat{\lambda}^k\langle\xi\rangle := \widehat{\lambda}^k\left(B^{k+\xi\alpha}\right)$. (Actually, you may think of $f^k\langle\xi\rangle := f^k(B^{k+\xi\alpha})$ for any family of functions f^k.)*

Lemma 3.6. *For $k > 0$ we now have the recursion*

$$\begin{aligned}\widetilde{\lambda}^k\langle\xi\rangle &= \alpha\int_0^1 \widetilde{\lambda}^{k-1}\langle\xi-\varrho\rangle\, B^{1+\varrho\alpha}\,\mathrm{d}\varrho,\\ \widehat{\lambda}^k\langle\xi\rangle &= \alpha\int_0^1 \widehat{\lambda}^{k-1}\langle\xi-\varrho\rangle\, B^{1+\varrho\alpha}\,\mathrm{d}\varrho\\ &\quad + 2\left(\widetilde{\lambda}^{k-1}+\widehat{\lambda}^{k-1}\right)\langle\xi\rangle\,\widehat{E}(B)\\ &\quad + \alpha\ln B\int_0^1 \left(\widetilde{\lambda}^{k-1}+\widehat{\lambda}^{k-1}\right)\langle\xi-\varrho\rangle\,\widehat{E}'(B^{1+\varrho\alpha})B^{1+\varrho\alpha}\,\mathrm{d}\varrho. \qquad \square\end{aligned}$$

4. Solving the recursion for $\widetilde{\lambda}^k$

To construct a useful description of the function $\widetilde{\lambda}^k$ we make a small excursion and consider the following family of piecewise polynomial functions.

Definition 4.1 (Polynomial hills). *Initially, define the integral operator $\mathcal{M}$ by*

$$(\mathcal{M}f)(\xi) = \int_0^1 f(\xi-\varrho)\,\mathrm{d}\varrho = \int_{\xi-1}^{\xi} f(\varrho)\,\mathrm{d}\varrho$$

*for any integrable function $f\colon \mathbb{R}\to\mathbb{R}$. Now for $k \in \mathbb{N}_{>1}$ let the k-*th polynomial hill *be*

$$\widetilde{m}^k := \mathcal{M}\widetilde{m}^{k-1}$$

based on the rectangular function $\widetilde{m}^1$ given by $\widetilde{m}^1(\xi) = 1$ for $\xi \in [0,1[$ and $\widetilde{m}^1(\xi) = 0$ otherwise.

Actually, $\widetilde{m}^1 = \mathcal{M}\widetilde{m}^0$ if we let $\widetilde{m}^0 = \delta$ be the 'left lopsided' Dirac delta distribution defined by its integral $\int_{-\infty}^{\xi} \delta(t)\ \mathrm{d}t$ being 0 for $\xi < 0$ and 1 for $\xi \geq 0$. Contrastingly, the standard Dirac delta function is balanced and has $\int_{-\infty}^{0} \delta(t)\ \mathrm{d}t = \frac{1}{2}$. However, we will stick to the lopsided variant throughout the entire paper. By $\mathcal{D}_\xi$ we denote the differential operator with respect to ξ .

Lemma 4.2 (Polynomial hills).

(i) $\widetilde{m}^k(\xi) = 0$ *for* $\xi < 0$ *or* $\xi \geq k$.

(ii) $\widetilde{m}^k(\xi) = \frac{1}{(k-1)!}\xi^{k-1}$ *for* $\xi \in [0, 1[$ *and* $\widetilde{m}^k(\xi) = \frac{1}{(k-1)!}(k-\xi)^{k-1}$ *for* $\xi \in [k-1, k[$.

(iii) $\widetilde{m}^k$ *restricted to* $[j, j+1[$ *is a polynomial function of degree* $k-1$ *for* $j \in \{0, \ldots, k-1\}$. *In particular,* $\widetilde{m}^k$ *is smooth for* $\xi \in \mathbb{R} \setminus \{0, \ldots, k\}$.

(iv) $\widetilde{m}^k$ *is* $(k-2)$*-fold continuously differentiable.*

(v) Conversely, the conditions (i) through (iv) uniquely determine $\widetilde{m}^k$.

(vi) $\mathcal{D}_\xi^i \widetilde{m}^k = \mathcal{M}\mathcal{D}_\xi^i \widetilde{m}^{k-1}$ *as long as* $i \leq k-2$ *and even for* $i = k-1$ *when read for distributions.*

(vii) The function $\widetilde{m}^k$ *is symmetric to* $\frac{k}{2}$: $\widetilde{m}^k(\xi) = \widetilde{m}^k(k-\xi)$.

(viii) For $\xi \in [j, j+1[$ *(corresponding to case* (k, j)*) we have*

$$\mathcal{D}_\xi^{k-1}\widetilde{m}^k(\xi) = (-1)^j \cdot \binom{k-1}{j}.$$

(ix) The next derivate can only be correctly described as a linear combination of Dirac delta distributions:

$$\mathcal{D}_\xi^{k}\widetilde{m}^k(\xi) = \sum_{0 \leq j \leq k} (-1)^j \binom{k}{j} \cdot \delta(\xi - j).$$

(x) For any $0 \leq \ell < k$ *we obtain the following explicit description:*

$$\mathcal{D}_\xi^{\ell}\widetilde{m}^k(\xi) = \frac{1}{(k-1-\ell)!} \sum_{0 \leq i \leq \lfloor \xi \rfloor} \binom{k}{i} (-1)^i (\xi - i)^{k-1-\ell}$$

(xi) Further, $\widetilde{m}^k(\xi) = \frac{\xi}{k-1}\widetilde{m}^{k-1}(\xi) + \frac{k-\xi}{k-1}\widetilde{m}^{k-1}(\xi - 1)$ *holds.*

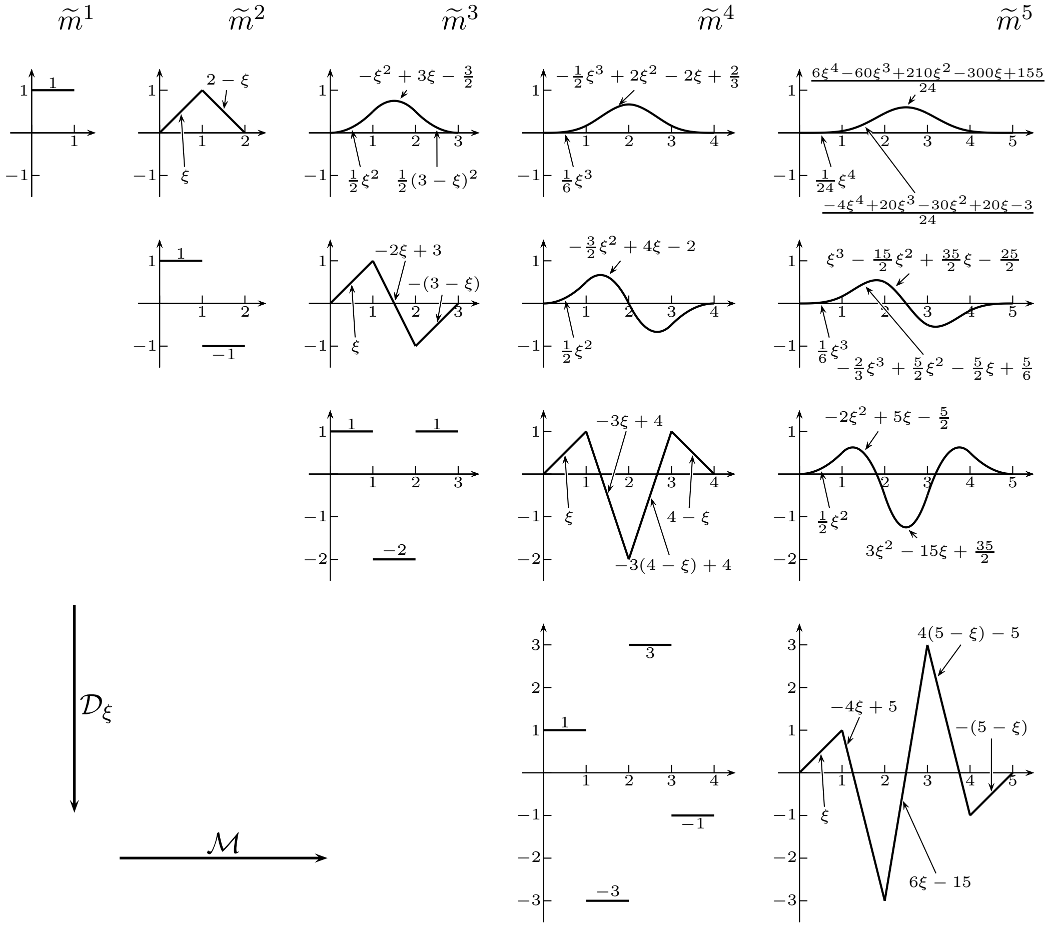


Figure 4.1: Graphs of the polynomial hills $\widetilde{m}^k$ for $k \leq 5$ and their derivatives

Curiosity: The function $\sqrt{k}\cdot\widetilde{m}^k$ can also be described as the volume of a slice through a $(k-1)$-dimensional unit hypercube of thickness $\frac{1}{\sqrt{k}}$ orthogonal to a main diagonal. That's the same as saying it is $\frac{1}{\sqrt{k}}$ times the $(k-1)$-volume of the cut between a k-dimensional hypercube and the hyperplane $\sum_{1\leq i\leq k} \varrho_i = \xi$. This last interpretation makes it obvious that

$$\int_0^k \widetilde{m}^k(\xi)\ \mathrm{d}\xi = 1,$$

since this is the volume of the k-hypercube.

Proof. From the definition (i) through (vii) follow directly. Further, note that $(\mathcal{M}\mathcal{D}_\xi f)(\xi) = f(\xi) - f(\xi-1)$. This is obvious from $(\mathcal{M}f)(\xi) = \int_{\xi-1}^{\xi} f(\varrho)\ \mathrm{d}\varrho$.

We prove (viii) by induction on k. For $k=1$ this is true by definition. So consider

$k > 1$. The recursion for $\widetilde{m}$ differentiated $k-1$ times yields for $\xi \in [j, j+1[$

$$\begin{aligned}\mathcal{D}_\xi^{k-1}\widetilde{m}^k(\xi) &= \mathcal{D}_\xi \mathcal{M}\mathcal{D}_\xi^{k-2}\widetilde{m}^{k-1}(\xi)\\ &= \mathcal{D}_\xi^{k-2}\widetilde{m}^{k-1}(\xi) - \mathcal{D}_\xi^{k-2}\widetilde{m}^{k-1}(\xi-1)\\ &= (-1)^j\binom{k-2}{j} - (-1)^{j-1}\binom{k-2}{j-1} = (-1)^j\binom{k-1}{j}.\end{aligned}$$

(ix) follows similarly.

To prove (x) consider $h(\xi) = \frac{1}{(k-1)!}\sum_{0\le i\le\lfloor\xi\rfloor}\binom{k}{i}(-1)^i(\xi-i)^{k-1}$. Then $\mathcal{D}_\xi^{k-1}h = \mathcal{D}_\xi^{k-1}\widetilde{m}^k$ using (viii). And obviously $\mathcal{D}_\xi^\ell h(0) = 0 = \mathcal{D}_\xi^\ell \widetilde{m}^k(0)$ for $0 \le \ell < k-1$, so that inductively (with falling ℓ) we get $\mathcal{D}_\xi^\ell h = \mathcal{D}_\xi^\ell \widetilde{m}^k$.

As we do not need (v) and (xi), we leave these proofs to the interested reader. □

Most of the following is easier if we first renormalize $\widetilde{\lambda}^k$. So we let

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle := \frac{1}{\alpha^k B^{k+\xi\alpha}}\widetilde{\lambda}^k\left\langle \xi \right\rangle. \tag{4.3}$$

The recursion for $\widetilde{\lambda}^k$ now turns into

$$\widetilde{\lambda}^k_{\text{norm}} = \mathcal{M}\widetilde{\lambda}^{k-1}_{\text{norm}}.$$

THEOREM 4.4 (Approximation order). *For any $\xi \in \mathbb{R}$ we have*

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle = \int_0^\xi B^{-\varrho\alpha}\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho = B^{-\xi\alpha}\int_0^\xi B^{\varrho\alpha}\widetilde{m}^k(\varrho)\,\mathrm{d}\varrho,$$

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle = \frac{1}{(-\alpha\ln B)^k}\left(\sum_{0\le i\le\lfloor\xi\rfloor}\binom{k}{i}(-1)^i B^{-(\xi-i)\alpha} - \sum_{0\le\ell\le k-1}(-\alpha\ln B)^\ell\cdot\mathcal{D}_\xi^{k-\ell-1}\widetilde{m}^k(\xi)\right),$$

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle = \sum_{0\le i\le\lfloor\xi\rfloor}\binom{k}{i}(-1)^i\frac{\operatorname{cutexp}_k\left(-(\xi-i)\alpha\ln B\right)}{(-\alpha\ln B)^k},$$

where $\operatorname{cutexp}_k(\zeta) = \exp(\zeta) - \sum_{0\le\ell\le k-1}\frac{\zeta^\ell}{\ell!} = \sum_{\ell\ge k}\frac{\zeta^\ell}{\ell!}$. *We can also express* cutexp_k *using the incomplete Gamma function* $\Gamma(k,\zeta) = \int_\zeta^\infty \mathrm{e}^{-\varrho}\varrho^{k-1}\,\mathrm{d}\varrho$ *by* $\operatorname{cutexp}_k(\zeta) = \exp(\zeta) - \frac{\Gamma(k,\zeta)}{\exp(-\zeta)\Gamma(k,0)}$.

Proof. The definition for $\widetilde{\lambda}^0$ turns into

$$\widetilde{\lambda}^0_{\mathrm{norm}}\left\langle \xi \right\rangle = \int_0^\infty B^{-\varrho\alpha}\delta(\xi-\varrho)\,\mathrm{d}\varrho\,.$$

Now, since $\mathcal{M}$ commutes with this integration this immediately implies that

$$\widetilde{\lambda}^k_{\mathrm{norm}}\left\langle \xi \right\rangle = \int_0^\infty B^{-\varrho\alpha}\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho$$

which is the first stated equality noting that $\widetilde{m}^k$ is zero outside $[0,k]$. By partial integration we obtain

$$\begin{aligned}\widetilde{\lambda}^k_{\mathrm{norm}}\left\langle \xi \right\rangle &= \frac{1}{\alpha\ln B}\widetilde{m}^k(\xi) - \frac{1}{\alpha\ln B}\int_0^\infty B^{-\varrho\alpha}\mathcal{D}_\xi\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho\\ &= \sum_{1\le i\le k}\frac{(-1)^{i-1}}{(\alpha\ln B)^i}\mathcal{D}_\xi^{i-1}\widetilde{m}^k(\xi) + \frac{(-1)^k}{(\alpha\ln B)^k}\int_0^\infty B^{-\varrho\alpha}\mathcal{D}_\xi^k\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho\,.\end{aligned}$$

Using the description of $\mathcal{D}_\xi^k\widetilde{m}^k$ from Lemma 4.2(ix) the last integral turns into the claimed sum of the second stated equality. Expressing $\mathcal{D}_\xi^{k-\ell-1}\widetilde{m}^k(\xi-\varrho)$ using Lemma 4.2(x) and rearranging slightly yields the third equality. □

We are going to estimate the estimation of the error in the next section. To that aim we first need to estimate $\widetilde{\lambda}^k_{\mathrm{norm}}$. If $k>0$ then, based on Theorem 4.4 and $\widetilde{m}^k(\xi)\le 1$, we obtain the upper bound

$$\widetilde{\lambda}^k_{\mathrm{norm}}\left\langle \xi \right\rangle = \int_0^\infty B^{-\varrho\alpha}\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho \le \frac{1}{\alpha\ln B}.$$

For $k=0$ we have $\widetilde{\lambda}^0_{\mathrm{norm}}\left\langle \xi \right\rangle = B^{-\xi\alpha}$ for $\xi\ge 0$ and so $\widetilde{\lambda}^0_{\mathrm{norm}}\left\langle \xi \right\rangle \le 1$ will do for all $\xi\in\mathbb{R}$.

We first describe the qualitative behaviour of $\widetilde{\lambda}^k_{\mathrm{norm}}$. Actually its graph looks like a slighty biaswise hill.

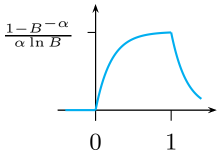
Lemma 4.5. *The function* $\widetilde{\lambda}^k_{\mathrm{norm}}\left\langle \xi \right\rangle = B^{-\xi\alpha}\int_0^\xi B^{\varrho\alpha}\widetilde{m}^k(\varrho)\,\mathrm{d}\varrho$ *is zero at* $\xi=0$*, positive at* $\xi=k$*, more precisely*

$$\widetilde{\lambda}^k_{\mathrm{norm}}\left\langle k \right\rangle = \left(\frac{1-B^{-\alpha}}{\alpha\ln B}\right)^k,$$

and there is a position $\xi^k_{\frac12}\in\,]0,k]$ *such that it is increasing on* $]0,\xi^k_{\frac12}[$ *and decreasing on* $]\xi^k_{\frac12},\xi[$*. Further,* $\xi^k_{\frac12}\ge\frac{k}{2}$*.*

Proof. First, inspecting

$$\begin{aligned}\widetilde{\lambda}^1_{\text{norm}}\left\langle \xi \right\rangle &= \int_0^\xi B^{-\varrho\alpha}\widetilde{m}^1(\xi-\varrho)\,\mathrm{d}\varrho\\ &= \begin{cases} 0 & \text{if } \xi < 0,\\ \frac{1-B^{-\xi\alpha}}{\alpha\ln B} & \text{if } \xi\in[0,1],\\ \frac{1-B^{-\alpha}}{\alpha\ln B}B^{-(\xi-1)\alpha} & \text{if } \xi>1.\end{cases}\end{aligned}$$



shows that for $k=1$ all claims hold with $\xi^k_{\frac{1}{2}}=1$. So in the remainder of this proof we assume $k>1$.

Next, compute $\widetilde{\lambda}^k_{\text{norm}}\left\langle k \right\rangle$ inductively:

$$\begin{aligned}\widetilde{\lambda}^k_{\text{norm}}\left\langle k \right\rangle &= B^{-k\alpha}\int_0^k B^{\varrho\alpha}\int_0^1 \widetilde{m}^{k-1}(\varrho-\varrho_k)\,\mathrm{d}\varrho_k\ \mathrm{d}\varrho\\ &= \underbrace{B^{-\alpha}\int_0^1 B^{\varrho_k\alpha}\,\mathrm{d}\varrho_k}_{=\frac{1-B^{-\alpha}}{\alpha\ln B}}\cdot\underbrace{B^{-(k-1)\alpha}\int_0^{k-1}B^{\tau\alpha}\widetilde{m}^{k-1}(\tau)\,\mathrm{d}\tau}_{=\widetilde{\lambda}^{k-1}_{\text{norm}}\left\langle k-1 \right\rangle} = \left(\frac{1-B^{-\alpha}}{\alpha\ln B}\right)^k.\end{aligned}$$

Here we have substituted $\tau=\varrho-\varrho_k$ and collapsed the new integration interval $[-\varrho_k, k-\varrho_k]$ for τ to $[0,k-1]$ since $\widetilde{m}^{k-1}$ vanishes on the difference Moreover, based on $\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle = B^{-\xi\alpha}\int_0^\xi B^{\varrho\alpha}\widetilde{m}^k(\varrho)\,\mathrm{d}\varrho$ we obtain

$$\mathcal{D}_\xi\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle = -\alpha\ln B\cdot\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle+\widetilde{m}^k(\xi), \tag{4.6}$$

and infer that $\mathcal{D}_\xi\widetilde{\lambda}^k_{\text{norm}}\left\langle k \right\rangle = -\alpha\ln B\left(\frac{1-B^{-\alpha}}{\alpha\ln B}\right)^k$ is negative.

Finally, compute the derivate of $\widetilde{\lambda}^k_{\text{norm}}$ differently

$$\mathcal{D}_\xi\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle = \mathcal{D}_\xi\left(\int_0^\xi B^{-\varrho\alpha}\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho\right) = B^{-\xi\alpha}\int_0^\xi B^{\varrho\alpha}\mathcal{D}_\xi\widetilde{m}^k(\varrho)\,\mathrm{d}\varrho\,.$$

The integral kernel $B^{\varrho\alpha}\mathcal{D}_\xi\widetilde{m}^k(\varrho)$ is positive on $]0,\frac{k}{2}[$ and negative on $]\frac{k}{2},k[$. Thus $\int_0^\xi B^{\varrho\alpha}\mathcal{D}_\xi\widetilde{m}^k(\varrho)\,\mathrm{d}\varrho$ increases on $]0,\frac{k}{2}[$ and decreases on $]\frac{k}{2},k[$. Since this term starts at zero, it is positive for some time, begins to decrease at $\frac{k}{2}$, traverses zero at some point $\xi^k_{\frac{1}{2}}$ recalling that at k the value is negative, and stays negative til $\xi=k$ since it continues to decrease. Thus the sign of $\mathcal{D}_\xi\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle$ is positive on $]0,\xi^k_{\frac{1}{2}}[$ and negative on $]\xi^k_{\frac{1}{2}},k[$, and so $\widetilde{\lambda}^k_{\text{norm}}\left\langle \xi \right\rangle$ is increasing till $\xi^k_{\frac{1}{2}}$ and decreasing afterwards. □

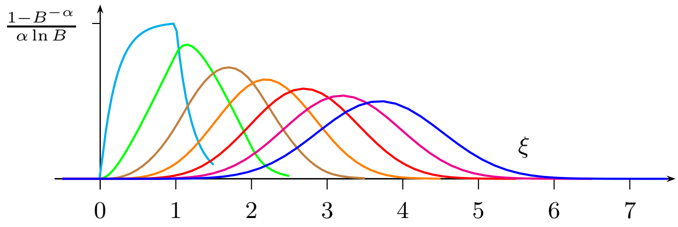


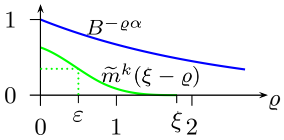
Figure 4.2: $\widetilde{\lambda}^k_{\text{norm}}\left\langle\xi\right\rangle$ for $\xi\in\left[-\frac12,k+\frac12\right]$ and $k=1,2,3,4,5,6,7$

LEMMA 4.7. *Assume $k\geq 2$, $\alpha\ln B\geq\frac{\ln 16}{k}$, and $\xi\in[0,1]$. Then we have*

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle\xi\right\rangle\geq\frac{\exp\left(-\frac{\ln^2 4}{\alpha\ln B}\right)}{\alpha\ln B}\cdot\frac{\xi^k}{k!}.$$

The assumptions are already true for $C=2B$ when $k\geq 4$. Note that this is rather sharp as for $\xi\in[0,1]$ we have $\widetilde{\lambda}^k_{\text{norm}}\left\langle\xi\right\rangle\leq\frac{\xi^k}{k!}$.

PROOF. We use the integral representation from Theorem 4.4 and estimate the polynomial hill part $\widetilde{m}^k(\xi-\varrho)$ of its kernel by a simple piecewise constant function as indicated in the picture. We obtain



$$\begin{aligned}\widetilde{\lambda}^k_{\text{norm}}\left\langle\xi\right\rangle&=\int_0^\xi B^{-\varrho\alpha}\widetilde{m}^k(\xi-\varrho)\,\mathrm{d}\varrho\\&\geq\int_0^\varepsilon B^{-\varrho\alpha}\,\mathrm{d}\varrho\cdot\widetilde{m}^k(\xi-\varepsilon)\\&=\frac{1}{\alpha\ln B}\left(1-\exp\left(-\varepsilon\alpha\ln B\right)\right)\widetilde{m}^k(\xi-\varepsilon).\end{aligned}$$

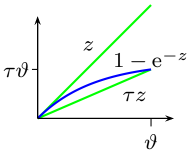
This holds for any $\varepsilon\in[0,\xi]$ since $0\leq\xi\leq\frac{k}{2}$ ensures that $\widetilde{m}^k$ is increasing. So we can optimize ε depending on ξ. We obtain a suitable value when setting ε by

$$1-\exp\left(-\varepsilon\alpha\ln B\right)=\frac{\xi}{k}. \tag{4.8}$$

To make sure that now $\varepsilon\leq\xi$ we use the following simple fact.

FACT 4.9. *For any $\vartheta>0$ and $\tau=\frac{1-\exp(-\vartheta)}{\vartheta}$ the map*

$$\begin{array}{rcl}[0,\vartheta]&\longrightarrow&[0,\tau\vartheta],\\ z&\longmapsto&1-\exp(-z),\end{array}$$



is bijective and increasing and for $z\in[0,\vartheta]$ we have $\tau z\leq 1-\exp(-z)\leq z$. △

Let $\vartheta_1 > 0$ be such that $1 - \exp(-\vartheta_1) = \frac{1}{k}$. Namely, $\vartheta_1 = -\ln\left(1 - \frac{1}{k}\right)$. With $\tau_1 = \frac{1-\exp(-\vartheta_1)}{\vartheta_1}$ then $1 = \tau_1\vartheta_1 k$ and $\frac{\xi}{k} \leq \tau_1\vartheta_1$. Thus we have $\varepsilon\alpha\ln B \in [0, \vartheta_1]$ so that

$$\tau_1\varepsilon\alpha\ln B \leq 1 - \exp(-\varepsilon\alpha\ln B) = \frac{\xi}{k} \leq \varepsilon\alpha\ln B. \tag{4.10}$$

In particular, $\varepsilon \leq \xi$ follows from $k\tau_1\alpha\ln B = \frac{1}{\vartheta_1}\alpha\ln B \geq 1$. By Fact 4.9 with $\vartheta = \ln 2$ we obtain $\tau = \frac{1}{2\ln 2}$ and $\left(1 - \frac{1}{k}\right)^k \geq \exp(-\frac{1}{\tau}) = \exp(-\ln 4)$ for all $k \geq 2$. Thus $k\vartheta_1 = -k\ln\left(1 - \frac{1}{k}\right) \leq \ln 4$. Further, $\alpha\ln B \geq \frac{\ln 16}{k} > \frac{\ln 4}{k} \geq \vartheta_1$. This now implies $\varepsilon \leq \xi$.

Since $\xi \in [0, 1]$ we have the explicit expression $\widetilde{m}^k(\xi - \varepsilon) = \frac{(\xi-\varepsilon)^{k-1}}{(k-1)!}$ and so

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle\xi\right\rangle \geq \frac{\xi}{k\alpha\ln B}\widetilde{m}^k(\xi - \varepsilon) = \frac{(1 - \varepsilon/\xi)^{k-1}}{\alpha\ln B} \cdot \frac{\xi^k}{k!}.$$

Since $\vartheta_1 < \alpha\ln B$ we can define ϑ_2 by $1 - \exp(-\vartheta_2) = \frac{\vartheta_1}{\alpha\ln B}$, and according to Fact 4.9 let $\tau_2 = \frac{1-\exp(-\vartheta_2)}{\vartheta_2}$. Combining with (4.10) gives us $\left(1 - \frac{\varepsilon}{\xi}\right)^k \geq \left(1 - \frac{1}{k\tau_1\alpha\ln B}\right)^k = \exp\left(-\frac{1}{\tau_2\tau_1\alpha\ln B}\right)$ and thus simplifies our above inequality to

$$\widetilde{\lambda}^k_{\text{norm}}\left\langle\xi\right\rangle \geq \frac{\exp\left(-\frac{1}{\tau_2\tau_1\alpha\ln B}\right)}{\alpha\ln B} \cdot \frac{\xi^k}{k!}. \tag{4.11}$$

By our choices

$$\frac{1}{\tau_1\tau_2\alpha\ln B} = k\vartheta_2 \geq \frac{k\vartheta_1}{\alpha\ln B} \geq \frac{1}{\alpha\ln B}.$$

Though these inequalities get equalities with $k \to \infty$, we need a precise estimate. Substituting k in $-k\ln\left(1 - \frac{1}{k}\right) \leq \ln 4$ with $\frac{k\alpha\ln B}{\ln 4}$ yields

$$\begin{aligned}\frac{1}{\tau_2\tau_1} &= k\alpha\ln B \cdot \vartheta_2 = -k\alpha\ln B\ln\left(1 - \frac{k\vartheta_1}{k\alpha\ln B}\right) \\ &\qquad\qquad \leq -\frac{k\alpha\ln B}{\ln 4}\ln\left(1 - \frac{\ln 4}{k\alpha\ln B}\right)\ln 4 \leq \ln^2 4\end{aligned}$$

provided $\alpha\ln B \geq \frac{\ln 16}{k}$. □

Though we know the value of $\widetilde{\lambda}^k_{\text{norm}}\left\langle k\right\rangle$, it is orders smaller than the above left lower bound. Thus let us consider $\widetilde{\lambda}^k_{\text{norm}}$ on $[k-1, k]$.

Lemma 4.12. *If $k \geq 3$ then for $\xi \in [k-1,k]$ we have*

$$\widetilde{\lambda}^k_{\text{norm}}\langle\xi\rangle \geq \frac{(1-B^{-\alpha})^k}{\alpha \ln B} \cdot \frac{(k-\xi)^{k-1}}{(k-1)!}.$$

Proof. By definition we have $\widetilde{\lambda}^k_{\text{norm}}\langle\xi\rangle = \frac{\widetilde{\lambda}^k\langle\xi\rangle}{\alpha^k B^{k+\xi\alpha}}$. Theorem 4.4's third description expresses $\widetilde{\lambda}^k_{\text{norm}}$ on $[k-1,k]$ as a sum of k terms. Adding the missing term $i=k$ we obtain $\frac{\widetilde{\lambda}^k\langle k\rangle}{\alpha^k B^{k+\xi\alpha}}$, noting that $\widetilde{\lambda}^k$ is constant for $\xi > k$:

$$\widetilde{\lambda}^k_{\text{norm}}\langle\xi\rangle = \left(\frac{1-B^{-\alpha}}{\alpha \ln B}\right)^k B^{(k-\xi)\alpha} - \frac{\operatorname{cutexp}_k((k-\xi)\alpha\ln B)}{(\alpha\ln B)^k}$$

To check the claimed inequality we substitute $\tau = (k-\xi)\alpha\ln B \in [0, \alpha\ln B]$ (eliminating ξ):

$$\widetilde{\lambda}^k_{\text{norm}}\langle\xi\rangle = \frac{\sum_{0\leq\ell\leq k-1}\frac{\tau^\ell}{\ell!} - \left(1-(1-B^{-\alpha})^k\right)\mathrm{e}^\tau}{(\alpha\ln B)^k}.$$

We have to show that this is at least $\frac{(1-B^{-\alpha})^k}{(\alpha\ln B)^k}\frac{\tau^{k-1}}{(k-1)!}$ which we rewrite to

$$\sum_{0\leq\ell\leq k-2}\frac{\tau^\ell}{\ell!} \geq \left(1-(1-B^{-\alpha})^k\right)\left(\mathrm{e}^\tau - \frac{\tau^{k-1}}{(k-1)!}\right).$$

Obviously $(1-B^{-\alpha})^k \geq (1-\mathrm{e}^{-\tau})^k$ in our situation, with equality for $\tau = \alpha\ln B$ or $\xi = k-1$. Thus it suffices to show for any $\tau > 0$

$$\sum_{0\leq\ell\leq k-2}\frac{\tau^\ell}{\ell!} \geq (1-(1-\mathrm{e}^{-\tau})^k)\left(\mathrm{e}^\tau - \frac{\tau^{k-1}}{(k-1)!}\right). \tag{4.13}$$

The remaining proof proceeds in four steps:

- High case: $\sum_{0\leq\ell\leq k-2}\frac{\tau^\ell}{\ell!} \geq k$.
- Low case: $\frac{1-\mathrm{e}^{-\tau}}{\tau} \geq \sqrt[k]{\frac{1+\sigma}{k!}}$, where $\frac{1}{\sigma}+1 \leq \frac{\mathrm{e}^{k-1}(k-1)!}{(k-1)^{k-1}}$.
- Covering: Fixing $\sigma := \frac{1}{\sqrt{2\pi(k-1)}-1}$ these cases cover all $\tau > 0$ if $k \geq 4$.
- Brute-force: Prove (4.13) for $k=3$. (Actually, for $k \in \{3,4,5,6,7,8,9\}$.)

High case: Since $\mathrm{e}^\tau \geq \sum_{0\leq\ell\leq k-2}\frac{\tau^\ell}{\ell!} \geq k$ in this case we have $\tau \geq \ln k$. Employing Bernoulli's inequality $(1-T)^k \geq 1-kT$ for $T = \mathrm{e}^{-\tau} \leq 1$ we obtain

$$\begin{aligned}(1-(1-\mathrm{e}^{-\tau})^k)\left(\mathrm{e}^\tau - \frac{\tau^{k-1}}{(k-1)!}\right) &\leq k\mathrm{e}^{-\tau}\left(\mathrm{e}^\tau - \frac{\tau^{k-1}}{(k-1)!}\right)\\ &= k\left(1-\frac{\tau^{k-1}}{(k-1)!}\mathrm{e}^{-\tau}\right) \leq k \leq \sum_{0\leq\ell\leq k-2}\frac{\tau^\ell}{\ell!}.\end{aligned}$$

As Bernoulli's inequality is good for T close to 0 only, it is not surprising that this only gives a sufficient result for τ large enough.

Low case: Assume $\frac{1-\mathrm{e}^{-\tau}}{\tau} \geq \sqrt[k]{\frac{1+\sigma}{k!}}$ where σ is chosen such that $\frac{1}{\sigma}+1 < \frac{\mathrm{e}^{k-1}(k-1)!}{(k-1)^{k-1}}$. (Since $\frac{1-\mathrm{e}^{-\tau}}{\tau}$ is decreasing, this is always true on some interval $[0, \tau_0]$.)

The condition on σ implies that $\mathrm{e}^{\tau} - \left(\frac{1}{\sigma}+1\right)\frac{\tau^{k-1}}{(k-1)!}$ is non-negative for all $\tau > 0$: Consider $f_0(\tau) = \frac{\mathrm{e}^{\tau}(k-1)!}{\tau^{k-1}} - \left(\frac{1}{\sigma}+1\right)$. Then f_0' vanishes at $\tau = k-1$ only and thus f_0 is minimal there. The assumption on σ is precisely $f_0(k-1) \geq 0$.

Further, note that $\frac{\tau^{k-2}}{(k-2)!} + \frac{\tau^{k-1}}{(k-1)!} \leq \mathrm{e}^{\tau} \leq \sum_{0\leq \ell\leq k-1} \frac{\tau^{\ell}}{\ell!} + \mathrm{e}^{\tau}\frac{\tau^k}{k!}$. We use this to obtain:

$$\begin{aligned}
&\Big(1 - \underbrace{(1-\mathrm{e}^{-\tau})^k}_{\geq \frac{(1+\sigma)\tau^k}{k!}}\Big) \underbrace{\left(\mathrm{e}^{\tau} - \frac{\tau^{k-1}}{(k-1)!}\right)}_{\geq 0} \\
&\leq \mathrm{e}^{\tau} - \frac{\tau^{k-1}}{(k-1)!} - (1+\sigma)\frac{\tau^k}{k!}\mathrm{e}^{\tau} + (1+\sigma)\frac{\tau^k}{k!}\frac{\tau^{k-1}}{(k-1)!} \\
&\leq \sum_{0\leq \ell\leq k-2} \frac{\tau^{\ell}}{\ell!} - \frac{\sigma\tau^k}{k!}\mathrm{e}^{\tau} + (1+\sigma)\frac{\tau^k}{k!}\frac{\tau^{k-1}}{(k-1)!} \\
&= \sum_{0\leq \ell\leq k-2} \frac{\tau^{\ell}}{\ell!} - \sigma\frac{\tau^k}{k!}\underbrace{\left(\mathrm{e}^{\tau} - \left(\frac{1}{\sigma}+1\right)\frac{\tau^{k-1}}{(k-1)!}\right)}_{\geq 0} \leq \sum_{0\leq \ell\leq k-2} \frac{\tau^{\ell}}{\ell!}.
\end{aligned}$$

Notice that the value of σ only influences the set of values of τ that fall in this case.

Covering: We choose $\sigma := \frac{1}{\sqrt{2\pi(k-1)}-1}$. Recall Stirling's formula: For any $n > 0$ there is a $\vartheta \in \,]0,1[$ such that $n! = \left(\frac{n}{\mathrm{e}}\right)^n \sqrt{2\pi n}\mathrm{e}^{\frac{1}{12n+\vartheta}}$, see Robbins (1955). We thus have $\frac{1}{\sigma}+1 = \sqrt{2\pi(k-1)} < \frac{\mathrm{e}^{k-1}(k-1)!}{(k-1)^{k-1}}$ as required. Further, we define the value τ_{split} where we split between the low and the high case:

$$\tau_{\text{split}} := \begin{cases} 2\ln\frac{k}{\mathrm{e}} & \text{if } k \geq 8, \\ 2 & \text{if } 5 \leq k \leq 7, \\ \sqrt{7}-1 & \text{if } k = 4. \end{cases}$$

We start with the treatment of the cases $k \geq 8$.

We claim that for $\tau \leq \tau_{\text{split}}$ we are in the low case, ie.

$$\frac{1-\mathrm{e}^{-\tau}}{\tau} \geq \sqrt[k]{\frac{1+\sigma}{k!}} =: \vartheta. \tag{4.14}$$

Consider $f_2(\tau) = 1 - \mathrm{e}^{-\tau} - \vartheta\tau$. It obviously vanishes at $\tau = 0$. The derivative of f_2 shows that there is exactly one maximum at $\tau = -\ln(\vartheta)$, which is roughly $\ln k$. To

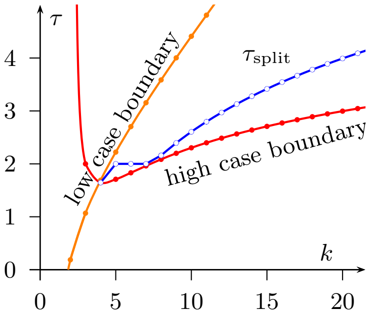


Figure 4.3: Case coverage and τ_{split}

prove (4.14) for $\tau \in]0, \tau_{\text{split}}]$ it is thus sufficient to prove that f_2 is at least 0 at the right boundary. First, note that by Stirling's formula we have $k! \geq \left(\frac{k}{\mathrm{e}}\right)^k \sqrt{2\pi}$ and so we can estimate ϑ by $\frac{\mathrm{e}}{k}$:

$$\vartheta = \sqrt[k]{\frac{1+\sigma}{k!}} \leq \frac{\mathrm{e}}{k} \sqrt[k]{\underbrace{\frac{2}{\sqrt{2\pi}}}_{\leq 1}} \leq \frac{\mathrm{e}}{k}.$$

Well, now we have

$$\begin{aligned} k \cdot f_2\left(\tau_{\text{split}}\right) &= k - \frac{\mathrm{e}^2}{k} - k\vartheta\tau_{\text{split}} \\ &\geq k - \frac{\mathrm{e}^2}{k} - 2\mathrm{e} \ln \frac{k}{\mathrm{e}} =: f_3(k). \end{aligned}$$

Checking that $f_3(\mathrm{e}) = 0$ and the derivative $f_3'(k) = (1 - \frac{\mathrm{e}}{k})^2$ is positive for $k > \mathrm{e}$ shows that $f_3(k) > 0$ for all $k \geq 3$. Thus for $\tau \leq \tau_{\text{split}}$ we are in the low case with the above choice of σ.

It remains to check that for $\tau \geq \tau_{\text{split}}$ we are in the high case. We use the Lagrange remainder estimate of the power series of the exponential function and again Stirling's formula to obtain

$$\sum_{0 \leq \ell \leq k-2} \frac{\tau^\ell}{\ell!} \geq \mathrm{e}^\tau \left(1 - \frac{\tau^{k-1}}{(k-1)!}\right) \geq \mathrm{e}^\tau \left(1 - \left(\frac{\mathrm{e}\tau}{k-1}\right)^{k-1}\right) =: f_5(k, \tau).$$

As the left hand side is increasing in $\tau > 0$ we consider the smallest τ in question: let $f_6(k) := f_5(k, \tau_{\text{split}})/k$. Therein,

$$\left(\frac{\mathrm{e}\tau_{\text{split}}}{k-1}\right)^{k-1} = \exp\left(-\underbrace{(k-1)}_{\text{(I)}} \underbrace{\left(-\ln 2 - 1 - \ln\ln \frac{k}{\mathrm{e}} + \ln(k-1)\right)}_{\text{(II)}}\right).$$

Observe that the term (I) is obviously positive and increasing for $k \geq 8$. The same is true for the term (II): its derivative $\frac{1}{k-1} - \frac{1}{k(\ln k - 1)}$ is positive for $k \geq \mathrm{e}^2 \approx 7.39⊤$ and the value of term (II) at e^2 is positive. Using this we infer that f_6 is increasing and positive. Checking $f_6(10) > 1$ ($f_6(10) \in \,]1.19, 1.20[$) now proves $\sum_{0 \leq \ell \leq k-2} \frac{\left(2 \ln \frac{k}{\mathrm{e}}\right)^\ell}{\ell!} \geq k$ for $k \geq 10$. For $k = 8$ and $k = 9$ we just verify this inequality directly.

It remains to consider $4 \leq k \leq 7$. Here we use individual seperation positions as defined above:

k	4	5	6	7	(8)	(9)	
τ_{split}	$\sqrt{7} - 1$	2	2	2	$2 \ln \frac{8}{\mathrm{e}}$	$2 \ln \frac{9}{\mathrm{e}}$	
$\frac{1-\mathrm{e}^{-\tau_{\text{split}}}}{\tau_{\text{split}}}$	0.49⊥	0.43⟘	0.43⟘	0.43⟘	0.40⊓	0.37⊓	$\vee$ for low case
$\sqrt[k]{\frac{1+\sigma}{k!}}$	0.48⟙	0.40⊤	0.35Ч	0.31Ч	0.28⊔	0.25Ч	
$\sum_{0 \leq \ell \leq k-2} \frac{\tau_{\text{split}}^\ell}{\ell!}$	4	6.33⟘	7.00⊥	7.27⟙	8.60⟘	10.93⟙	$\geq k$ for high case

Just check that for this τ_{split} the low and the high case conditions are both fulfilled. Summing up: the claim is proved for $k \geq 4$.

$k < 10$: For $k = 3$ we *need* an explicit check as the estimates done in the low and the high case are too sloppy. As the following actually is a general computational way to verify the inequality (4.13) we do describe it in general, show computational results for $3 \leq k \leq 10$ and make the critical case $k = 3$ hand-checkable at the end. For the verification we use a small trick and brute force: First, we substitute occurrences of $\mathrm{e}^{-\tau}$ with a new variable T. The task turns into showing that the bivariate polynomial

$$F_k(\tau, T) := \sum_{0 \leq \ell \leq k-2} \frac{\tau^\ell}{\ell!} - \frac{(1 - (1-T)^k)}{T} \left(1 - \frac{\tau^{k-1}}{(k-1)!} T\right)$$

is non-negative at $\tau = -\ln T$ for $T \in \,]0, 1]$. Now, observe that F_k is increasing in $\tau > 0$ for fixed $T \in [0, 1]$. If we thus replace $-\ln T$ with a lower bound and we can show that the resulting term is still non-negative then we are done. For $T \in \,]0, 1]$ we have $-\ln T \geq \sum_{1 \leq \ell \leq s} \frac{(1-T)^\ell}{\ell}$. This lower bound even converges to $-\ln T$, which actually ensures that we can always find some s that allows the following reduction. We consider the univariate polynomial

$$g_{k,s}(T) := F_k\left(\sum_{1 \leq \ell \leq s} \frac{(1-T)^\ell}{\ell}, T\right).$$

By our reasoning, the claim follows if $\forall T \in \,]0, 1] : g_{k,s}(T) \geq 0$ for some s. This in turn is implied by

$$g_{k,s}(0) > 0 \quad \wedge \quad g_{k,s}(T) \text{ has no zero for } 0 < T < 1. \tag{4.15}$$

The second statement can be checked using Sturm's theorem (Sturm 1835) by only evaluating certain rational polynomials at $T = 0$ and $T = 1$. However, this only works if the chosen s is large enough. We have determined the smallest s that make (4.15) true:

k	3	4	5	6	7	(8)	(9)
s	4	3	4	5	6	7	8
$\deg g_{k,s}$	11	13	21	31	43	57	73
time (sec)	0.19	0.29	0.60	2.8	24	235	1704

Though we can always divide out $(1-T)^k$ from $g_{k,s}$ the degrees are in all cases quite high and the computations better done by a computer. The timings refer to our own (non-optimized) MuPad-program used to assert (4.15). As $k = 3$ is the only case that we do not cover otherwise we give $g_{3,4}$ here:

$$\begin{aligned} g_{3,4}(T)/(1-T)^3 = {} & \frac{1}{12}(1-T) + \frac{5}{6}T + T(1-T)\Bigg(\\ & \frac{481}{96}(1-T)^2 + \frac{35}{24}T^2 + T(1-T)\Bigg(\\ & \frac{245}{96}(1-T) + \frac{103}{24}T + T(1-T)\Bigg(\\ & \frac{119}{144}(1-T)^2 + \frac{89}{144}T^2 + T(1-T)\cdot\frac{407}{288}\Bigg)\Bigg)\Bigg) \end{aligned}$$

With this description you can easily see that it is positive on $[0,1[$. □

Finally, we put together the upper bound on $\widetilde{\lambda}^k_{\text{norm}}$, Lemma 4.5, Lemma 4.7, and Lemma 4.12 in the following theorem.

THEOREM 4.16. *For any $k \geq 1$ we have*

$$\widetilde{\lambda}^k_{\text{norm}}\langle\xi\rangle \leq \tilde{c}_k := \begin{cases} \frac{1}{\alpha\ln B} & \text{if } k > 0, \\ 1 & \text{if } k = 0. \end{cases}$$

Assume $\alpha\ln B \geq \max\left(\ln 2, \frac{\ln 16}{k}\right)$. Then for any $\varepsilon \in\ ]0,1]$ with $\varepsilon \leq k - \xi^k_{\frac{1}{2}}$ or $k < 3$ there is a $\breve{c}_k > 0$ such that for $\xi \in [\varepsilon, k-\varepsilon]$

$$\widetilde{\lambda}^k_{\text{norm}}\langle\xi\rangle \geq \frac{\breve{c}_k}{\alpha\ln B}.$$

Here we can choose

$$\breve{c}_k = \min\left(2^{-4}\cdot\frac{\varepsilon^k}{k!},\quad 2^{-k}\cdot\frac{\varepsilon^{k-1}}{(k-1)!} \right).$$

Note that $\xi^k_{\frac{1}{2}}$ is the maximum of $\widetilde{\lambda}^k_{\text{norm}}$ which in our experiments is always less then $k-1$ for $k \geq 3$. However, proving that would result in a stronger version of Lemma 4.12, which even in the given form required quite some effort. However, we just want that to work for some small ε and that is always granted.

PROOF. The upper bound being proven we consider the lower bound. First, keeping in mind that $\alpha \ln B \geq \ln 2$ and $\alpha \ln B \geq \frac{\ln 16}{k}$, we consider the cases $k \geq 3$. We know by Lemma 4.5 that $\widetilde{\lambda}^k_{\text{norm}}$ on $[\varepsilon, k-\varepsilon]$ attains its minimal value at one of the boundaries since $\xi^k_{\frac{1}{2}} \in [\varepsilon, k-\varepsilon]$ (by assumption). We thus only need to consider its values at $\xi = \varepsilon$ and at $\xi = k - \varepsilon$.

On the left hand side Lemma 4.7 gives

$$\alpha \ln B \cdot \widetilde{\lambda}^k_{\text{norm}} \langle \varepsilon \rangle \geq \exp\left(-\frac{\ln^2 4}{\alpha \ln B}\right) \frac{\varepsilon^k}{k!} \geq \exp\left(-\frac{\ln^2 4}{\ln 2}\right) \frac{\varepsilon^k}{k!} = 2^{-4} \cdot \frac{\varepsilon^k}{k!}$$

using the conditions on $\alpha \ln B$.

On the right hand side by Lemma 4.12 we find

$$\alpha \ln B \cdot \widetilde{\lambda}^k_{\text{norm}} \langle k - \varepsilon \rangle \geq (1 - \exp(-\alpha \ln B))^k \frac{\varepsilon^{k-1}}{(k-1)!} \geq 2^{-k} \frac{\varepsilon^{k-1}}{(k-1)!}$$

using again $\alpha \ln B \geq \ln 2$. This completes the proof for the cases $k \geq 3$.

We will now show corresponding lower bounds for the cases $k = 1, 2$. For $k = 1$ we have for $\varepsilon \in]0, 1]$ using $\alpha \ln B \geq \ln 2$:

$$\alpha \ln B \cdot \widetilde{\lambda}^1_{\text{norm}} \langle \varepsilon \rangle = 1 - \exp(-\varepsilon \alpha \ln B) \geq 1 - \exp(-\varepsilon \ln 2).$$

Using Fact 4.9 and $\varepsilon \leq 1$, we have

$$1 - \exp(-\varepsilon \ln 2) \geq \frac{1 - \exp(-\ln 2)}{\ln 2} \varepsilon = \frac{1}{2 \ln 2} \varepsilon \geq \frac{1}{2} \varepsilon.$$

For $k = 2$ we again apply Lemma 4.7 for the left hand side as in the general case. For the right hand side we show that

$$\alpha^2 \ln^2 B \cdot \widetilde{\lambda}^2_{\text{norm}} \langle 2 - \varepsilon \rangle \geq \left(1 - \frac{1}{2 \ln 2}\right) \varepsilon \alpha \ln B$$

for $0 \leq \varepsilon \alpha \ln B \leq \alpha \ln B$, $\ln 2 \leq \alpha \ln B$. Since $\left(1 - \frac{1}{2 \ln 2}\right) \geq 2^{-2}$ this proves the claim. Now, using Theorem 4.4 we write the left hand side minus the right hand side as $f_5(\varepsilon \alpha \ln B, \alpha \ln B)$ with $f_5(\tau, \vartheta) = \exp(\tau - 2\vartheta) - 2 \exp(\tau - \vartheta) + \frac{1}{2 \ln 2} \tau + 1$. We have to show that f_5 is non-negative if $0 \leq \tau \leq \vartheta$ and $\vartheta \geq \ln 2$. The ϑ-derivative of f_5,

$$\frac{\partial f_5}{\partial \vartheta}(\tau, \vartheta) = 2 \exp(-\vartheta)(1 - \exp(-\vartheta)) \exp(\tau),$$

is positive for $\vartheta > 0$. Thus it suffices to show that $f_5(\tau, \vartheta) \geq 0$ for the smallest allowed ϑ, which is the larger of τ and $\ln 2$. If $\tau \geq \ln 2$ then we consider $f_5(\tau, \tau) = \exp(-\tau) + \frac{1}{2\ln 2}\tau - 1$. This expression is increasing in this case (even for $\tau \geq \ln 2 + \ln\ln 2$) and so it is greater than or equal to $f_5(\ln 2, \ln 2) = 0$. If otherwise $0 \leq \tau \leq \ln 2$ then we consider $f_5(\tau, \ln 2) = -\frac{3}{4}\exp(\tau) + \frac{1}{2\ln 2}\tau + 1$ which is decreasing even for $\tau \geq 0$ and so it is greater than or equal to $f_5(\ln 2, \ln 2) = 0$. □

Summing up we obtain:

Corollary 4.17. *For any $\varepsilon \in \,]0,1]$ and any $k \geq 1$ we have uniformly for $\xi \in [\varepsilon, k - \varepsilon]$*

$$\widetilde{\lambda}^k_{\text{norm}} \left\langle \xi \right\rangle \in \Theta\left(\frac{1}{\alpha \ln B}\right). \qquad \square$$

5. Estimating the estimate $\widehat{\lambda}^k$

The recurrence Lemma 3.6 for $\widehat{\lambda}^k$ is more complex than the one for $\widetilde{\lambda}^k$, so instead of solving it we estimate it. We consider also here the normed version $\widehat{\lambda}^k_{\text{norm}} \left\langle \xi \right\rangle := \frac{\widehat{\lambda}^k \langle \xi \rangle}{\alpha^k B^{k+\xi\alpha}}$. To better understand how the error behaves we compute it for $k = 1$:

$$\widehat{\lambda}^1_{\text{norm}} \left\langle \xi \right\rangle = \begin{cases} 0 & \text{if } \xi \in \,]-\infty, 0[, \\ \frac{1+\xi\alpha}{8\pi\alpha} \frac{\ln B}{B^{\frac{1}{2}+\frac{\xi\alpha}{2}}} + \frac{1}{8\pi\alpha} \frac{\ln B}{B^{\frac{1}{2}+\xi\alpha}} & \text{if } \xi \in [0, 1[, \\ \frac{1+\alpha}{8\pi\alpha} \frac{\ln B}{B^{\frac{1}{2}-\frac{\alpha}{2}+\xi\alpha}} + \frac{1}{8\pi\alpha} \frac{\ln B}{B^{\frac{1}{2}+\xi\alpha}} & \text{if } \xi \in [1, \infty[. \end{cases}$$

From this we estimate $\widehat{\lambda}^1_{\text{norm}}$ directly:

$$\widehat{\lambda}^1_{\text{norm}} \left\langle \xi \right\rangle \leq \begin{cases} 0 & \text{if } \xi \in \,]-\infty, 0[, \\ \frac{(2+\alpha)\ln B}{8\pi\alpha} B^{-\frac{1+\xi\alpha}{2}} & \text{if } \xi \in [0, 1[, \\ \frac{(1+\alpha)\ln B}{8\pi\alpha} B^{-\frac{1}{2}+\frac{\alpha}{2}-\xi\alpha} + \frac{\ln B}{8\pi\alpha} \cdot B^{-\frac{1}{2}-\xi\alpha} & \text{if } \xi \in [1, \infty[. \end{cases}$$

We have also looked at precise expressions for larger k, yet they are huge and do not give rise to better bounds.

Theorem 5.1. *Define values $\widehat{c}_k$ recursively by*

$$\widehat{c}_k := \widehat{c}_{k-1} + \frac{4 + 3\ln B}{8\pi\alpha\sqrt{B}} \left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right)$$

for $k \geq 3$ based on $\widehat{c}_0 := 0$, $\widehat{c}_1 := \frac{(2+\alpha)\ln B}{8\pi\alpha\sqrt{B}}$, and

$$\begin{aligned} \widehat{c}_2 &:= \frac{6 + 3\alpha}{8\pi\alpha^2} \frac{1}{\sqrt{B}} + \frac{4 + 3\ln B}{8\pi\alpha\sqrt{B}} \left(\widetilde{c}_1 + \widehat{c}_1\right) \\ &= \frac{9 + 3\alpha}{8\pi\alpha^2} \frac{1}{\sqrt{B}} + \frac{1}{2\pi\alpha^2\sqrt{B}\ln B} + \frac{(2+\alpha)(4 + 3\ln B)\ln B}{64\pi^2\alpha^2 B}. \end{aligned}$$

Then for any k and $\xi \in \mathbb{R}$ we have

$$\widehat{\lambda}^k_{\text{norm}} \langle \xi \rangle \leq \widehat{c}_k$$

If $\alpha \geq \frac{\ln B}{\sqrt{B}}$ we have for $k \geq 2$ and large B the inequality

$$\widehat{c}_k \leq \frac{(2^k - 1)(1+\alpha)}{\alpha^2 \sqrt{B}}.$$

For $k = 1$ the order of $\widehat{c}_1$ is necessarily slightly larger. More precisely, we have for large B that

$$\widehat{c}_1 \leq \frac{(1+\alpha)\ln B}{\alpha \sqrt{B}}.$$

Instead of defining $\widehat{c}_2$ and $\widehat{c}_1$ we could have left that to the recursion. But the given values are smaller than the ones derived from the recursion based on $\widehat{c}_0$ only. For $k = 1$ the recursion would give $\frac{4+3\ln B}{8\pi\alpha\sqrt{B}}$. For $k \geq 2$ however the improvement due to these explicit settings is a factor of order $\ln B$.

Proof. We first show that the value $\widehat{c}_k$ is bounded as claimed. For $k = 1$ the claim follows directly from the definition, since we have for $B > \exp(1)$ that $(2+\alpha)\ln B \leq 2(1+\alpha)\ln B$ as α is positive. For $k = 2$ we have for $\ln^2 B \leq \sqrt{B}$ the inequality

$$\begin{aligned}
\widehat{c}_2 &= \frac{6+3\alpha}{8\pi\alpha^2}\frac{1}{\sqrt{B}} + \frac{4+3\ln B}{8\pi\alpha\sqrt{B}}\left(\widetilde{c}_1 + \widehat{c}_1\right) \\
&\leq \frac{1+\alpha}{\alpha^2\sqrt{B}} + \frac{1}{\alpha^2\sqrt{B}} + \frac{(1+\alpha)\ln^2 B}{\alpha^2 B} \\
&\leq \frac{3(1+\alpha)}{\alpha^2\sqrt{B}}.
\end{aligned}$$

For $k \geq 2$ we proceed inductively. We have

$$\begin{aligned}
\widehat{c}_k &= \widehat{c}_{k-1} + \frac{4+3\ln B}{8\pi\alpha\sqrt{B}}\left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right) \\
&\leq \frac{(2^{k-1}-1)(1+\alpha)}{\alpha^2\sqrt{B}} + \frac{\ln B}{\alpha\sqrt{B}}\left(\frac{1}{\alpha \ln B} + \frac{(2^{k-1}-1)(1+\alpha)}{\alpha \ln B}\right) \\
&= \frac{(2^k-1)(1+\alpha)}{\alpha^2\sqrt{B}}.
\end{aligned}$$

Now we prove the remaining estimate by induction on k. The case $k = 0$ is true by definition of $\widehat{\lambda}^0$ (with equality). For $k = 1$ the inspection above proves the claim. The explicit calculation of $\widehat{\lambda}^1$ also shows that a bound of order $\mathcal{O}\left({}^{x}/\sqrt{B}\right)$ is impossible. We defer the case $k = 2$ to the end of the proof as most of it will be as in the general case. So assume $k \geq 3$. Using the definition of $\widehat{\lambda}^k$ from Lemma 3.6 we split $\widehat{\lambda}^k$ into three summands:

$$\begin{aligned}\widehat{\lambda}^k_{\mathrm{norm}} \langle \xi \rangle = & \int_0^1 \widehat{\lambda}^{k-1}_{\mathrm{norm}} \langle \xi - \varrho \rangle \ \mathrm{d}\varrho \\ & + \frac{2\widehat{E}(B)}{\alpha B} \cdot (\widetilde{\lambda}^{k-1}_{\mathrm{norm}} + \widehat{\lambda}^{k-1}_{\mathrm{norm}}) \langle \xi \rangle \\ & + \int_0^1 (\widetilde{\lambda}^{k-1}_{\mathrm{norm}} + \widehat{\lambda}^{k-1}_{\mathrm{norm}}) \langle \xi - \varrho \rangle \ \widehat{E}'(B^{1+\varrho\alpha}) \ln B \ \mathrm{d}\varrho \, .\end{aligned}$$

For $\widehat{E}(x) = \frac{1}{8\pi}\sqrt{x}\ln x$ we calculate as a preparative

$$\frac{2\widehat{E}(B)}{\alpha B} = \frac{\ln B}{4\pi\alpha\sqrt{B}}, \tag{5.2}$$

$$\int_0^1 \widehat{E}'(B^{1+\varrho\alpha}) \ln B \ \mathrm{d}\varrho = \frac{4 + \ln B}{8\pi\alpha\sqrt{B}} - \frac{4 + \ln C}{8\pi\alpha\sqrt{C}}. \tag{5.3}$$

The first summand of $\widehat{\lambda}^k_{\mathrm{norm}}$ is at most $\widehat{c}_{k-1}$ by induction hypothesis. The second summand we estimate using (5.2) by

$$\frac{\ln B}{4\pi\alpha\sqrt{B}} \left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right).$$

The third summand is bounded by

$$\left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right) \int_0^1 \widehat{E}'(B^{1+\varrho\alpha}) \ln B \ \mathrm{d}\varrho \, .$$

By (5.3) the third summand is at most

$$\frac{4 + \ln B}{8\pi\alpha\sqrt{B}} \left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right).$$

This completes the proof of the case $k \geq 3$:

$$\begin{aligned}\widehat{\lambda}^k_{\mathrm{norm}} \langle \xi \rangle & \leq \widehat{c}_{k-1} + \frac{\ln B}{4\pi\alpha\sqrt{B}} \left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right) + \frac{4 + \ln B}{8\pi\alpha\sqrt{B}} \left(\widetilde{c}_{k-1} + \widehat{c}_{k-1}\right) \\ & = \widehat{c}_k .\end{aligned}$$

For $k = 2$ we have to improve the estimate of the first summand only, since the other terms anyways are of order at most $\mathcal{O}\left(1/\sqrt{B}\right)$. For $\xi < 0$ there is nothing to prove. For $\xi \in [0,1[$ we find for this first summand

$$\begin{aligned}
\int_0^{\xi} \widehat{\lambda}^1_{\text{norm}}\left\langle \xi-\varrho \right\rangle \,\mathrm{d}\varrho &\leq \int_0^{\xi} \frac{(2+\alpha)\ln B}{8\pi\alpha} B^{-\frac{1}{2}-\frac{(\xi-\varrho)\alpha}{2}} \,\mathrm{d}\varrho \\
&= \frac{(2+\alpha)\ln B}{8\pi\alpha} B^{-\frac{1}{2}} \underbrace{B^{-\frac{\xi\alpha}{2}} \int_0^{\xi} B^{\frac{\varrho\alpha}{2}} \,\mathrm{d}\varrho}_{=\frac{2}{\alpha\ln B}\left(1-B^{-\frac{\xi\alpha}{2}}\right)} \\
&\leq \frac{2+\alpha}{4\pi\alpha^2\sqrt{B}}.
\end{aligned}$$

For $\xi \in [1,2]$ we find

$$\begin{aligned}
\int_0^{1} \widehat{\lambda}^1_{\text{norm}}\left\langle \xi-\varrho \right\rangle \,\mathrm{d}\varrho \leq{}& \int_{\xi-1}^{1} \frac{(2+\alpha)\ln B}{8\pi\alpha} B^{-\frac{1}{2}-\frac{(\xi-\varrho)\alpha}{2}} \,\mathrm{d}\varrho \\
&+ \int_0^{\xi-1} \widehat{\lambda}^1_{\text{norm}}\left\langle 1 \right\rangle B^{1+\alpha} B^{-(1+(\xi-\varrho)\alpha)} \,\mathrm{d}\varrho \\
={}& \frac{(2+\alpha)\ln B}{8\pi\alpha} B^{-\frac{1}{2}-\frac{(\xi-1)\alpha}{2}} \underbrace{B^{-\frac{\alpha}{2}} \int_{\xi-1}^{1} B^{\frac{\varrho\alpha}{2}} \,\mathrm{d}\varrho}_{=\frac{2}{\alpha\ln B}\left(1-B^{-\frac{(2-\xi)\alpha}{2}}\right)} \\
&+ \widehat{\lambda}^1_{\text{norm}}\left\langle 1 \right\rangle \underbrace{B^{-(\xi-1)\alpha} \int_0^{\xi-1} B^{\varrho\alpha} \,\mathrm{d}\varrho}_{=\frac{1}{\alpha\ln B}\left(1-B^{-(\xi-1)\alpha}\right)} \\
\leq{}& \frac{2+\alpha}{4\pi\alpha^2} B^{-\frac{1}{2}-\frac{(\xi-1)\alpha}{2}} + \frac{1+\alpha}{8\pi\alpha^2} B^{-\frac{1}{2}-\frac{\alpha}{2}} + \frac{1}{8\pi\alpha^2} B^{-\frac{1}{2}-\alpha} \\
\leq{}& \frac{6+3\alpha}{8\pi\alpha^2\sqrt{B}}
\end{aligned}$$

As $\widehat{\lambda}^1_{\text{norm}}$ decreases for $\xi \geq 1$ this bound also holds for $\xi \geq 2$. Putting everything together the above defined value $\widehat{c}_2$ bounds $\widehat{\lambda}^2_{\text{norm}}\left\langle \xi \right\rangle$ as claimed. □

It is tempting to guess that we can save more $\ln B$ factors for larger k. However, inspecting $\widehat{\lambda}^2_{\text{norm}}$ shows that, say, $\widehat{\lambda}^3_{\text{norm}}\left\langle \frac{1}{2} \right\rangle \in \Omega\left(\frac{1}{\sqrt{B}}\right)$. (For $\xi \in [0,1[$ we find $\widehat{\lambda}^2_{\text{norm}}\left\langle \xi \right\rangle = \frac{3}{4\pi\alpha\sqrt{B}} + \mathcal{O}\left(\frac{1}{\sqrt{B}\ln B}\right)$.)

6. Reestimating $\widehat{\lambda}^k$ without Riemann

If you do not want to assume the Riemann hypothesis then only weaker bounds $\widehat{E}(x)$ on $|\pi(x) - \operatorname{Li}(x)|$ can be used. In Ford (2002a,b) we found the following explicit bounds, the first one he attributes to a paper by Y. Cheng which we could not find.

Fact 6.1. ○ *For $x > 10$ we have*

$$|\pi(x) - \mathrm{Li}(x)| \leq 11.88\,x(\ln x)^{\frac{3}{5}} \exp\left(-\frac{1}{57}(\ln x)^{\frac{3}{5}}(\ln\ln x)^{-\frac{1}{5}}\right).$$

○ *There is a constant C and a frontier x_0 such that for $x > x_0$ we have*

$$|\pi(x) - \mathrm{Li}(x)| \leq C\,x \exp\left(-0.2098(\ln x)^{\frac{3}{5}}(\ln\ln x)^{-\frac{1}{5}}\right).$$

Admittedly, these bounds only start to be meaningful at large values of x (eg. the first statement around $10^{159\,299}$). All those bounds are of the form: For all $x > x_0$

$$|\pi(x) - \mathrm{Li}(x)| \leq \underbrace{C\,x\,(\ln x)^{c_0} \exp\left(-A\,(\ln x)^{c_1}(\ln\ln x)^{-c_2}\right)}_{=:\widehat{E}(x)}$$

holds. Here, $C > 0$, $x_0 > 0$, $c_0 \in \mathbb{R}$, $c_1 > 0$, $c_2 > 0$ and $A > 0$ are given parameters (which are not always known). Note that we have that

$$\widehat{E}(x)/_x$$

is decreasing for large x. Actually, with the parameter sets from Fact 6.1 this is already true for $x \geq 5$. Moreover, the quotient of the relative errors at $x^{1+\alpha}$ and at x

$$\frac{\widehat{E}(x^{1+\alpha})\frac{\ln x^{1+\alpha}}{x^{1+\alpha}}}{\widehat{E}(x)\frac{\ln x}{x}} = \frac{(1+\alpha)\widehat{E}(x^{1+\alpha})}{x^{\alpha}\widehat{E}(x)}$$

is bounded (or even tends to zero) with $x \to \infty$ for any $\alpha > 0$. This follows from $\widehat{E}(x)/_x$ decreasing when α is constant, but you may also consider values for α that increase when x grows.

Revisiting the proof of Theorem 5.1 shows that only (5.2), (5.3), and the initial values $\widehat{c}_1$ and $\widehat{c}_2$ depend on the specific bound $\widehat{E}$. We now use the following recursion for the bounds:

$$\widehat{c}_k := \widehat{c}_{k-1} + \underbrace{\left(\frac{2\widehat{E}(B)}{\alpha B} + \int_0^1 \widehat{E}'(B^{1+\varrho\alpha}) \ln B \;\mathrm{d}\varrho\right)}_{=:u}(\widetilde{c}_{k-1} + \widehat{c}_{k-1})$$

for $k \geq 1$ based on $\widehat{c}_0 = 0$, and possibly values for $\widehat{c}_1$ and $\widehat{c}_2$.

To bound u tightly the trickiest step is bounding the integral. As our interests lie elsewhere we take the easy way out. We integrate by parts and use that $\widehat{E}(x)/_x$ is decreasing for the following rough estimate

$$\int_0^1 \widehat{E}'(B^{1+\varrho\alpha}) \ln B \;\mathrm{d}\varrho = \frac{\widehat{E}(B^{1+\alpha})}{\alpha B^{1+\alpha}} - \frac{\widehat{E}(B)}{\alpha B} + \ln B \underbrace{\int_0^1 \frac{\widehat{E}(B^{1+\varrho\alpha})}{B^{1+\varrho\alpha}} \;\mathrm{d}\varrho}_{\leq \frac{\widehat{E}(B)}{B}}.$$

Thus u is bounded by

$$u \leq \left(1 + \frac{1}{\alpha \ln B} \left(1 + \underbrace{\frac{\widehat{E}(B^{1+\alpha})}{B^\alpha \widehat{E}(B)}}_{\text{bounded}}\right)\right) \frac{\widehat{E}(B) \ln B}{B}.$$

In the following we neglect the bounded term, as we can compensate its effect for example by a small additional factor. Since u is small for large B, we expect $\widehat{c}_k$ to be dominated by $\widehat{c}_1 = u$. Precisely, for $k > 1$ we have $\widehat{c}_k = (1+u)\widehat{c}_{k-1} + \frac{u}{\alpha \ln B}$, thus

$$\widehat{c}_k = (1+u)^{k-1} u + \frac{(1+u)^{k-1} - 1}{\alpha \ln B} \sim \left(1 + \frac{k-1}{\alpha \ln B}\right) u.$$

Theorem 6.2. *Assume that $\widehat{E}(x)$ bounds $|\pi(x) - \mathrm{Li}(x)|$ and $\widehat{E}(x)/x$ is decreasing for $x > x_0$ and the relative error decreases fast, ie.*

$$\frac{\widehat{E}(x^{1+\alpha}) \frac{\ln x^{1+\alpha}}{x^{1+\alpha}}}{\widehat{E}(x) \frac{\ln x}{x}} = \frac{(1+\alpha)\widehat{E}(x^{1+\alpha})}{x^\alpha \widehat{E}(x)}$$

is bounded under the chosen behavior of α. Then for any $k \geq 2$ and B large we have

$$\widehat{\lambda}^k_{\mathrm{norm}} \langle \xi \rangle \in \mathcal{O}\left(\left(1 + \frac{k-1}{\alpha \ln B}\right)\left(1 + \frac{1}{\alpha \ln B}\right) \frac{\widehat{E}(B) \ln B}{B}\right)$$

for $k \geq 2$. □

This is close to optimal, we only loose a factor of order $\ln B$ in the relative error compared to the used error bound in the prime number theorem:

$$\frac{\widehat{\lambda}^k_{\mathrm{norm}} \langle \xi \rangle}{\widetilde{\lambda}^k_{\mathrm{norm}} \langle \xi \rangle} \leq \frac{\left(1 + \frac{k-1}{\alpha \ln B}\right)\left(1 + \frac{1}{\alpha \ln B}\right) \frac{\widehat{E}(B) \ln B}{B}}{\frac{\check{c}_k}{\alpha \ln B}} \sim \frac{\alpha}{\check{c}_k} \ln B \cdot \frac{\widehat{E}(B) \ln B}{B}.$$

The assumptions on $\widehat{E}$ also hold for explicit error bounds with $\widehat{E}(x) \in \mathcal{O}\left(\frac{x}{\ln^\ell x}\right)$. Due to the lost $\ln B$ the result is only meaningful if $\ell \geq 3$, so Rosser & Schoenfeld (1962) does not suffice. From Dusart (1998) we can use $\widehat{E}(x) = 2.3854 \frac{x}{\ln^3 x}$ for $x > 355\,991$, and obtain

$$\widehat{\lambda}^k_{\mathrm{norm}} \langle \xi \rangle \in \mathcal{O}\left(\frac{1}{\ln B}\right).$$

7. Improvements

We have a look at the quality of Theorem 3.5 when applied to our inspiring application. There $B = 1100 \cdot 10^6$, $C = 2^{37} - 1$, $\alpha = \ln(C)/\ln(B) - 1 = 0.232\overline{1}$, and the largest k of interest is $k = 4$. For these parameters we find

$$\left[\frac{1}{(1+\alpha)^k}, 1\right] \subset [0.434, 1]\,.$$

That is a great loss when we try to enclose the function of interest in a small interval. Actually, we can improve the theorem for the price of a slightly more complicated recursion. The present result was based on approximating $\mathring{\kappa}(\varrho) = \frac{1}{\ln p}$ for $p = B^{1+\varrho\alpha} \in\,]B, C]$ by $\mathring{\lambda}(\varrho) = \frac{1}{\ln B}$ in the recursion of Definition 3.1:

$$\widetilde{\kappa}^k_{B,C}\langle\xi\rangle = \alpha \ln B \int_B^C \widetilde{\kappa}^{k-1}_{B,C}\langle\xi - \varrho\rangle \cdot \mathring{\kappa}(\varrho) B^{1+\varrho\alpha}\,\mathrm{d}\varrho\,.$$

We get a better bound by using

$$\mathring{\nu}(\varrho) = \frac{1-\varrho}{\ln B} + \frac{\varrho}{\ln C}$$

with $p = B^{1+\varrho\alpha}$ instead.

Definition 7.1. *For $x \geq 0$ we let $\widetilde{\nu}^0 := \kappa^0_{B,C}$, and recursively for $k > 0$*

$$\widetilde{\nu}^k\langle\xi\rangle := \alpha \ln B \int_0^1 \widetilde{\nu}^{k-1}\langle\xi - \varrho\rangle \left(\frac{1-\varrho}{\ln B} + \frac{\varrho}{\ln C}\right) B^{1+\varrho\alpha}\,\mathrm{d}\varrho\,.$$

Theorem 7.2. *Write $C = B^{1+\alpha}$ and fix $k \in \mathbb{N}_{>0}$. Then for $x \in \mathbb{R}_{>0}$ we have*

$$\widetilde{\kappa}^k_{B,C}(x) \in \left[\left(\frac{1+\alpha}{(1+\frac{\alpha}{2})^2}\right)^k, 1\right] \widetilde{\nu}^k(x)\,. \qquad \square$$

In the light of the inspiring application we now find

$$\left[\left(\frac{1+\alpha}{(1+\frac{\alpha}{2})^2}\right)^k, 1\right] \subset [0.957, 1].$$

When we started to think about solving the recursion in Definition 7.1 our first trial was to reuse the polynomial hills $\widetilde{m}^k$. Yet, that didn't want to fit nicely. Instead we learned from our calculations that an exponential density instead of a linear one would be easier to connect to the polynomial hills. So we tried to approximate like this and got

$$\mathring{\kappa}(\varrho) = \frac{1}{\ln p} = \frac{1}{(1-\varrho)\ln B + \varrho \ln C} \approx \mathrm{e}^{-\ln\ln B - \varrho\ln(1+\alpha)} =: \mathring{\eta}(\varrho).$$

The exponent in $\mathring{\eta}$ is chosen such that for $\varrho = 0$ and $\varrho = 1$ we have equality. It turns out that this approximation is even better than the one before and at the same time easier to handle. Thus we replace the functions $\widetilde{\nu}^k$ with another family $\widetilde{\eta}^k$:

Definition 7.3. *For $\xi \in \mathbb{R}$ we let $\widetilde{\eta}^0 := \kappa^0_{B,C}$, and recursively for $k > 0$*

$$\widetilde{\eta}^k \left\langle \xi \right\rangle := \alpha \ln B \int_0^1 \widetilde{\eta}^{k-1} \left\langle \xi - \varrho \right\rangle \underbrace{\frac{(1+\alpha)^{-\varrho}}{\ln B}}_{=\mathring{\eta}(\varrho)} B^{1+\varrho\alpha} \, \mathrm{d}\varrho \, .$$

Theorem 7.4. *Write $C = B^{1+\alpha}$ and fix $k \in \mathbb{N}_{>0}$. Then for $x \in \mathbb{R}_{>0}$ we have*

$$\widetilde{\kappa}^k_{B,C}\left(x\right) \in \left[\left(\frac{\ln(1+\alpha)}{\alpha} (1+\alpha)^{\frac{1}{\ln(1+\alpha)} - \frac{1}{\alpha}} \right)^k, 1 \right] \widetilde{\eta}^k\left(x\right).$$

Proof. To prove this we have to relate the function $\mathring{\kappa}\colon [0,1] \to \mathbb{R}_{>0}$, $\varrho \mapsto 1/\ln\left(B^{1+\varrho\alpha}\right)$ occurring in the definition of $\widetilde{\kappa}^k_{B,C}$ to the function $\mathring{\eta}\colon [0,1] \to \mathbb{R}_{>0}$, $\varrho \mapsto \mathring{\eta}(\varrho)$ replacing it in the definition of $\widetilde{\eta}^k$. Routine calculus shows that the function $\mathring{\kappa}/\mathring{\eta}$ is at most 1, namely at $\varrho = 0$ and $\varrho = 1$, and assumes its minimum value $\frac{\ln(1+\alpha)}{\alpha}(1+\alpha)^{\frac{1}{\ln(1+\alpha)}-\frac{1}{\alpha}}$ at $\varrho = \frac{\alpha - \ln(1+\alpha)}{\alpha + \ln(1+\alpha)}$. □

Testing this with the parameters $\alpha = 0.232\overline{1}$ and $k = 4$ from our inspiring application we obtain

$$\left[\left(\frac{\ln(1+\alpha)}{\alpha} (1+\alpha)^{\frac{1}{\ln(1+\alpha)} - \frac{1}{\alpha}} \right)^k, 1 \right] \subset [0.978, 1].$$

To get a better impression we have plotted the lower interval boundary as a function of α for all three cases in Figure 7.1. We see that for small values of α we obtain good approximations of $\widetilde{\kappa}_{B,C}$ and all our attempts give only weak results for large α, but the one with $\mathring{\eta}$ is always best.

If we now rewrite the recursion to one for

$$\widetilde{\eta}^k_{\mathrm{norm}} \left\langle \xi \right\rangle = \frac{\widetilde{\eta}^k \left\langle \xi \right\rangle}{\alpha^k B^{k+\xi\alpha}(1+\alpha)^{-\xi}} = \frac{\widetilde{\eta}^k \left\langle \xi \right\rangle}{\alpha^k B^{k+\xi\left(\alpha - \frac{\ln(1+\alpha)}{\ln B}\right)}}$$

we find that $\widetilde{\eta}^k_{\mathrm{norm}} = \mathcal{M}\widetilde{\eta}^{k-1}_{\mathrm{norm}}$. So we'll obtain the solution from the polynomial hills as in Theorem 4.4 for $\widetilde{\lambda}^k$:

$$\widetilde{\eta}^k_{\mathrm{norm}} \left\langle \xi \right\rangle = \int_0^\infty \mathrm{e}^{-\varrho(\alpha \ln B - \ln(1+\alpha))} \, \widetilde{m}^k(\xi - \varrho) \, \mathrm{d}\varrho \, .$$

The only difference is that instead of α we have $\alpha - \frac{\ln(1+\alpha)}{\ln B}$. With this replacement Theorem 4.4 becomes:

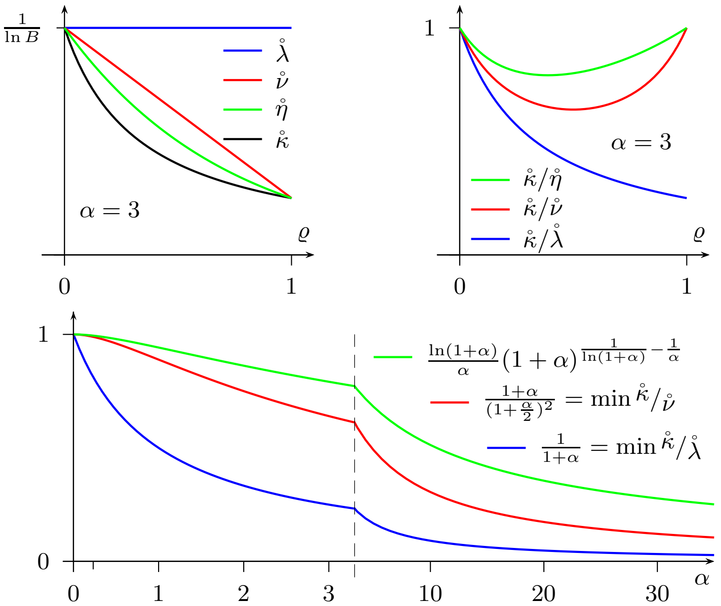


Figure 7.1: Comparing the quality of $\widetilde{\lambda}$, $\widetilde{\nu}$, $\widetilde{\eta}$: the top pictures show the integral kernels and their ratios for a specific α, the lower pictures show the minimum of the ratios as a function of α

Theorem 7.5. *For any $\xi \in \mathbb{R}$ we have*

$$\begin{aligned}
\widetilde{\eta}^k_{\text{norm}}\left\langle \xi \right\rangle &= \int_0^\xi B^{-\varrho\left(\alpha - \frac{\ln(1+\alpha)}{\ln B}\right)} \widetilde{m}^k(\xi - \varrho)\,\mathrm{d}\varrho \\
&= B^{-\xi\left(\alpha - \frac{\ln(1+\alpha)}{\ln B}\right)} \int_0^\xi B^{\varrho\left(\alpha - \frac{\ln(1+\alpha)}{\ln B}\right)} \widetilde{m}^k(\varrho)\,\mathrm{d}\varrho\,, \\
&= \int_0^\xi \left(\frac{B^\alpha}{1+\alpha}\right)^{-\varrho} \widetilde{m}^k(\xi - \varrho)\,\mathrm{d}\varrho \\
&= B^{-\xi\left(\alpha - \frac{\ln(1+\alpha)}{\ln B}\right)} \int_0^\xi \Bigg(\underbrace{\frac{B^\alpha}{1+\alpha}}_{=\frac{C/\ln C}{B/\ln B}}\Bigg)^{\varrho} \widetilde{m}^k(\varrho)\,\mathrm{d}\varrho\,,
\end{aligned}$$

$$\begin{aligned}\widetilde{\eta}^{k}_{\text{norm}}\left\langle \xi \right\rangle = {} & \frac{1}{(-\alpha \ln B + \ln(1+\alpha))^k} \\ & \left(\sum_{0 \le i \le \lfloor \xi \rfloor} \binom{k}{i} (-1)^i B^{-(\xi - i)\left(\alpha - \frac{\ln(1+\alpha)}{\ln B}\right)} \right. \\ & \left. - \sum_{0 \le \ell \le k-1} (-\alpha \ln B + \ln(1+\alpha))^{\ell} \cdot \mathcal{D}_{\xi}^{k-\ell-1} \widetilde{m}^{k}(\xi) \right),\end{aligned}$$

$$\widetilde{\eta}^{k}_{\text{norm}}\left\langle \xi \right\rangle = \sum_{0 \le i \le \lfloor \xi \rfloor} \binom{k}{i} (-1)^i \frac{\operatorname{cutexp}_k\left(-(\xi - i)\left(\alpha \ln B - \ln(1+\alpha)\right)\right)}{(-\alpha \ln B + \ln(1+\alpha))^k},$$

where $\operatorname{cutexp}_k(\zeta) = \exp(\zeta) - \sum_{0 \le \ell \le k-1} \frac{\zeta^\ell}{\ell!} = \sum_{\ell \ge k} \frac{\zeta^\ell}{\ell!}$.

8. Non-squarefree numbers are negligible

Considering $\kappa^{k}_{B,C}(x)$ we immediately observe that the ordering of the counted prime lists are not important and we can group together many such elements. To get a precise picture, we define the *sorting* of a tuple $P = (p_1, \ldots, p_k)$ in the following way:

$$S(P) := \Big(\{ j \le k \,|\, \operatorname{rank}_j P = i \} \Big)_{i \le k},$$

where $\operatorname{rank}_j P = \# \{ p_\ell \,|\, \ell \le k \wedge p_\ell \le p_j \}$. Now the count $\kappa^{k}_{B,C}(x)$ can be partitioned using the sets

$$A_S(x) := \left\{ P = (p_1, \ldots, p_k) \in (\mathbb{P} \cap]B, C])^k \;\middle|\; \begin{matrix} n = p_1 \ldots p_k \le x, \\ S(P) = S \end{matrix} \right\},$$

namely $\kappa^{k}_{B,C}(x) = \sum_S \# A_S(x)$ where S runs over all possible sortings. The above intuition would imply that many of these sets are essentially equal. We group them by their *type*

$$T(S) := (\# S_i)_{i \le k}.$$

Given any type $T = (T_1, \ldots, T_r)$, there are exactly $\binom{k}{T} = \frac{k!}{T_1! \cdots T_r!}$ different sortings S of type T. This corresponds to possible reorderings of a specific vector $P \in A_S(x)$ for a sorting S of type T. The type of such a vector P is defined to be $T(S)$. It is clear that the type of P is invariant under permutations, yet not its sorting.

Lemma 8.1. *Let T be a type for k elements.*

(i) There exists a sorting $S(T)$ of type T such that all vectors in $A_{S(T)}(x)$ are increasing.

(ii) If $T(S) = T$ then there is a permutation σ of k elements such that for all x we have $A_S(x) = A_{S(T)}(x)^\sigma$.

(iii) More precisely, for any sorting S of k elements the following are equivalent:

(a) $T(S) = T$.

(b) $\exists\sigma\colon S = S(T)^\sigma$.

(c) $\exists\sigma\colon \forall x\colon A_S(x) = A_{S(T)}(x)^\sigma$. □

Noting that $\#\{S \mid T(S) = T\} = \binom{k}{T}$ we have

$$\kappa^k_{B,C}(x) = \sum_T \sum_{S\colon T(S)=T} \#A_S(x) = \sum_T \binom{k}{T} \#A_{S(T)}(x)$$

On the other hand we have $\pi^k_{B,C}(x) = \sum_T 1 \cdot \#A_{S(T)}(x)$. In particular, we can deduce

$$\pi^k_{B,C}(x) < \kappa^k_{B,C}(x) \le k! \cdot \pi^k_{B,C}(x).$$

Actually, for large B (and C and x) we have $\pi^k_{B,C}(x) \sim \frac{1}{k!}\kappa^k_{B,C}(x)$. This stems from the following fact that $\#A_S(x)$ is asymptotically much smaller than $\#A_{S(1,\ldots,1)}(x)$ for any sorting S of k elements of type different from $(1,\ldots,1)$.

Lemma 8.2. *For any sorting S of k elements of type different from $(1,\ldots,1)$ there is a sorting S' of $k-1$ elements such that we have $\#A_S(x) \le \#A_{S'}(x/B) \le \frac{x}{B}$.*

Proof. Take S as specified. Let t be a position which does not occur as a singleton in S. Further, say $t \in S_\tau$, and let $r = \#S_\tau \ge 2$. Let S^- be the sorting with S_τ removed, and S' the sorting with t removed. (Retaining the old indexing is easier, yet then indices run over $\{1,\ldots,k\} \setminus S_\tau$, or $\{1,\ldots,k\} \setminus \{t\}$, respectively.) Then

$$\#A_S(x) = \sum_{p_t \in \mathbb{P} \cap]B,C]} \#A'_{S^-}(x/p_t^r) \le \sum_{p_t \in \mathbb{P} \cap]B,C]} \#A'_{S^-}(x/p_t B) = \#A_{S'}(x/B).$$

Here, A' denotes a variant of A consisting of prime vectors where at the positions j which should have smaller primes than p_t originally still satisfy that, and same for positions with primes larger than p_t. For the inequality note that $S^- = (S')^-$. Since obviously $\#A_S(z) \le z$ we are done. □

Combining this with $\sum_S \#A_S(x) = \kappa^k_{B,C}(x) \sim \widetilde{\kappa}^k_{B,C}(x) \in \Theta\left(\frac{x}{\ln B}\right)$, shows that there must be a large summand, which can be only $\#A_{S(1,\ldots,1)}(x)$.

The number $s(k) = \sum_T \binom{k}{T}$ of sortings of k elements is called ordered Bell number. We can also recursively define them: $s(0) = 1$, $s(k) = \sum_{0 \le r \le k-1} \binom{k}{r} s(r)$. According to Wilf (1994), page 175f, we have $s(k) = \frac{k!}{2\ln^{k+1} 2} + \mathcal{O}\left((0.16)^k k!\right)$. In particular, $s(k)$ is small in comparison to $2^{k-1}k!$. Using Lemma 8.2 for a comparison yields the — now immediate — following

Lemma 8.3. *We have*

$$\left|\pi^k_{B,C}(x) - \frac{1}{k!}\kappa^k_{B,C}(x)\right| \le \left(2^{k-1} - \frac{s(k)}{k!}\right)\frac{x}{B} < 2^{k-1}\frac{x}{B}.$$

Proof. $\left|k! \cdot \pi^k_{B,C}(x) - \kappa^k_{B,C}(x)\right| \le \sum_T \left(k! - \binom{k}{T}\right)\frac{x}{B} = \left(k!2^{k-1} - s(k)\right)\frac{x}{B}$. □

Compared to the error bound in $\left|\kappa^k_{B,C}(x) - \widetilde{\kappa}^k_{B,C}(x)\right| \le \widehat{\kappa}^k_{B,C}(x) \in \mathcal{O}(\frac{x}{\sqrt{B}})$ this is negligible when B is large. Here we assume $k \ge 2$ since the present observations are irrelevant for $k = 1$, namely $\pi^1_{B,C} = \kappa^1_{B,C}$.

9. Results on coarse-grained integers

We are going to combine the results of the last section with Theorem 4.16 and Theorem 5.1 to finally arrive at our main theorem.

Analogously to Definition 3.1, we define an approximation function for the function $\pi^k_{B,C}(x)$.

Definition 9.1. *For $x \ge 0$ and $k \ge 0$ we define*

$$\widetilde{\pi}^k_{B,C}(x) := \frac{1}{k!}\widetilde{\kappa}^k_{B,C}(x) \ \text{ and } \widehat{\pi}^k_{B,C}(x) := \frac{1}{k!}\widehat{\kappa}^k_{B,C}(x) + 2^{k-1}\frac{x}{B}.$$

Similarly to Definition 3.1 we can also recursively define $\widetilde{\pi}^k_{B,C}(x)$ by

$$\widetilde{\pi}^0_{B,C}(x) = \begin{cases} 0 & \text{if } x < 1, \\ 1 & \text{if } 1 \le x, \end{cases} \qquad \widetilde{\pi}^k_{B,C}(x) = \frac{1}{k}\int_B^C \frac{\widetilde{\pi}^{k-1}_{B,C}(x/p_k)}{\ln p_k}\,\mathrm{d}p_k\,.$$

It is also possible to define $\widehat{\pi}^k_{B,C}(x)$ similarly based on Definition 3.1. We can now describe the behavior of $\pi^k_{B,C}$ nicely and give our main result.

Theorem 9.2. *Given $x \in \mathbb{R}_{>0}$ and $k \in \mathbb{N}$. Then the inequality*

$$\left|\pi^k_{B,C}(x) - \widetilde{\pi}^k_{B,C}(x)\right| \le \widehat{\pi}^k_{B,C}(x)$$

holds.

Proof. By Lemma 8.3 we have

$$\left|\pi^k_{B,C}(x) - \frac{1}{k!}\kappa^k_{B,C}(x)\right| < 2^{k-1}\frac{x}{B}.$$

Thus using the triangle inequality and Theorem 3.2, we obtain

$$\left|\pi^k_{B,C}(x) - \frac{1}{k!}\widetilde{\kappa}^k_{B,C}(x)\right| < \frac{1}{k!}\widehat{\kappa}^k_{B,C}(x) + 2^{k-1}\frac{x}{B},$$

which proves the claim. □

THEOREM 9.3. *Fix $k \geq 2$. Then for any $\varepsilon > 0$ and B tending to infinity, there are for $x \in \left[B^k(1+\varepsilon), C^k(1-\varepsilon)\right]$ values $\widetilde{s}, \widehat{s} \in \left[\frac{1}{(1+\alpha)^k}, 1\right]$ such that*

$$\widetilde{\pi}^k_{B,C}(x) = \frac{\widetilde{s}}{k!}\widetilde{\lambda}^k(x), \qquad \widehat{\pi}^k_{B,C}(x) = \frac{\widehat{s}}{k!}\widehat{\lambda}^k(x) + 2^{k-1}\frac{x}{B}.$$

PROOF. By Definition 9.1 we have

$$\widetilde{\pi}^k_{B,C}(x) = \frac{1}{k!}\widetilde{\kappa}^k_{B,C}(x).$$

Theorem 3.5 tells us that there is a value $\widetilde{s} \in \left[\frac{1}{(1+\alpha)^k}, 1\right]$ such that

$$\widetilde{\kappa}^k_{B,C}(x) = \widetilde{s}\widetilde{\lambda}^k(x),$$

implying that for the same value $\widetilde{s}$ we have

$$\widetilde{\pi}^k_{B,C}(x) = \frac{\widetilde{s}}{k!}\widetilde{\lambda}^k(x).$$

Considering $\widehat{\pi}^k_{B,C}(x)$ we have by Definition 9.1 that

$$\widehat{\pi}^k_{B,C}(x) = \frac{1}{k!}\widehat{\kappa}^k_{B,C}(x) + 2^{k-1}\frac{x}{B}.$$

Applying Theorem 3.5 gives a value $\widehat{s} \in \left[\frac{1}{(1+\alpha)^k}, 1\right]$ such that

$$\widehat{\kappa}^k_{B,C}(x) = \widehat{s}\widehat{\lambda}^k(x),$$

which directly gives

$$\widehat{\pi}^k_{B,C}(x) = \frac{\widehat{s}}{k!}\widehat{\lambda}^k(x) + 2^{k-1}\frac{x}{B}.$$

This proves the theorem. □

Unrolling our results on $\widetilde{\lambda}^k(x)$ and $\widehat{\lambda}^k(x)$, namely Theorem 4.16 and Theorem 5.1, gives a slightly weaker result.

THEOREM 9.4. *Let $B < C = B^{1+\alpha}$ with $\alpha \geq \frac{\ln B}{\sqrt{B}}$ and fix $k \geq 2$. Then for any (small) $\varepsilon > 0$ and B tending to infinity we have for $x \in \left[B^k(1+\varepsilon), C^k(1-\varepsilon)\right]$ a value $\widetilde{a} \in \left[\frac{\alpha^{k-1}\breve{c}_k}{k!(1+\alpha)^k}, \frac{1}{k!}\right]$ with $\breve{c}_k = \min\left(2^{-4}\frac{\varepsilon^k}{k!}, 2^{-k}\frac{\varepsilon^{k-1}}{(k-1)!}\right)$ such that*

$$\left|\pi^k_{B,C}(x) - \widetilde{a}\frac{x}{\ln B}\right| \leq (2^k-1)\alpha^{k-2}(1+\alpha)\cdot\frac{x}{\sqrt{B}} + 2^{k-1}\frac{x}{B}.$$

PROOF. By Theorem 9.3 we have values $\widetilde{s}, \widehat{s} \in \left[\frac{1}{(1+\alpha)^k}, 1\right]$ such that

$$\widetilde{\pi}^k_{B,C}(x) = \frac{\widetilde{s}}{k!}\widetilde{\lambda}^k(x), \qquad \widehat{\pi}^k_{B,C}(x) = \frac{\widehat{s}}{k!}\widehat{\lambda}^k(x) + 2^{k-1}\frac{x}{B}.$$

By Theorem 4.16 we have for ε small enough that

$$\widetilde{\lambda}^k(x) \in [\breve{c}_k, 1]\,\frac{\alpha^{k-1}x}{\ln B}$$

and by Theorem 5.1 that

$$\widehat{\lambda}^k(x) \leq (2^k - 1)\alpha^{k-2}(1+\alpha) \cdot \frac{x}{\sqrt{B}}.$$

This gives the claim. □

10. Numeric evaluation

To discuss the quality of our results we consider again the example parameters $B = 1100 \cdot 10^6$, $C = 2^{37} - 1$, $\alpha = \ln(C)/\ln(B) - 1 = 0.232\overline{1}$, $k = 4$ from our inspiring application. For $k = 2$, $k = 3$ we can give similar pictures; of course, the errors are even smaller in these cases. At present we do not have efficient algorithms for computing $\kappa^k_{B,C}$ itself. However, based on our estimates we can compute values for encapsulating intervals in three variants, listed in increasing quality:

- λ estimate (Theorem 3.5):

$$\left[\frac{1}{(1+\alpha)^k}\widetilde{\lambda}^k(x) - \widehat{c}_k\alpha^k x, \quad \widetilde{\lambda}^k(x) + \widehat{c}_k\alpha^k x\right].$$

- η estimate (Theorem 7.4):

$$\left[\left(\frac{\ln(1+\alpha)}{\alpha}(1+\alpha)^{\frac{1}{\ln(1+\alpha)} - \frac{1}{\alpha}}\right)^k \widetilde{\eta}^k(x) - \widehat{c}_k\alpha^k x, \quad \widetilde{\eta}^k(x) + \widehat{c}_k\alpha^k x\right].$$

- κ estimate (Theorem 3.2):

$$\left[\widetilde{\kappa}^k_{B,C}(x) - \widehat{\kappa}^k_{B,C}(x), \quad \widetilde{\kappa}^k_{B,C}(x) + \widehat{\kappa}^k_{B,C}(x)\right].$$

The κ estimate was easiest to obtain and is of course the most accurate one, however, it is difficult to evaluate. The λ estimate was easy to obtain and compute. But it is of course the least accurate of the three. The η estimate was slightly more difficult to find, is as easy to evaluate as the prior, and it is much more accurate. As usual we write $x = B^{k+\xi\alpha}$ and use ξ as a running parameter.

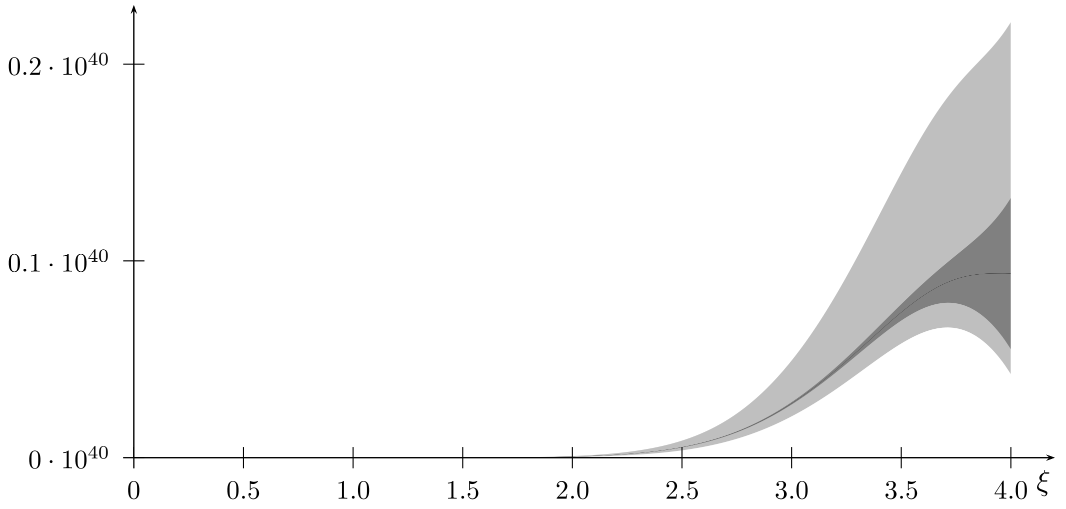


Figure 10.1: Absolute behavior of the estimates for $\kappa^k_{B,C}\langle\xi\rangle$. The light gray area shows the λ estimate, the dark gray area the η estimate, and the black area (well, yes) shows the κ estimate. The parameters are $B = 1100 \cdot 10^6$, $C = 2^{37} - 1$, $\alpha = \ln(C)/\ln(B) - 1 = 0.232\overline{1}$, $k = 4$.

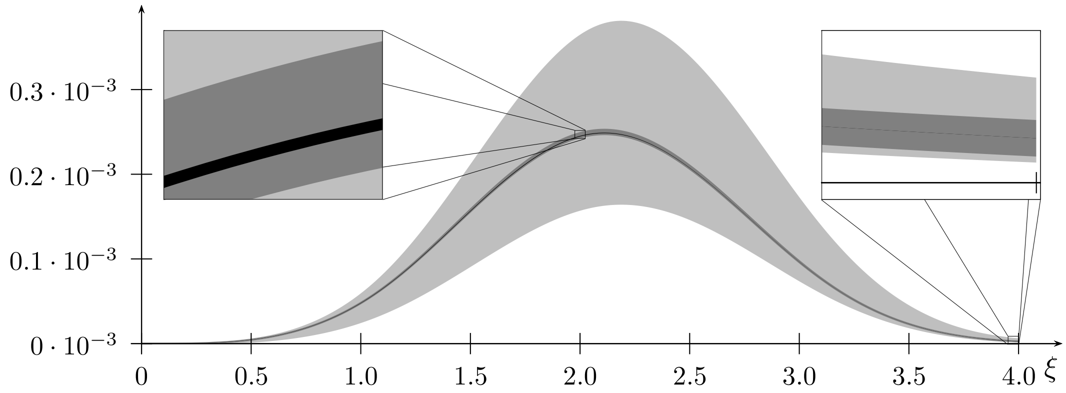


Figure 10.2: Behavior of the estimates relative to $x = B^{k+\xi\alpha}$. Colors and parameters are as in Figure 10.1.

Figure 10.1 shows the absolute behavior of all estimates. We observe that the absolute errors at the right margin are huge. This is expected as also the error estimates in the prime number theorem only bound the relative error. However, the picture completely conceals information about the middle and the left part of the interval $[0, k]$.

To see more we divide by $x = B^{k+\xi\alpha}$ and therefore obtain estimates for the ratio of $]B, C]$-grained integers x in Figure 10.2. This reveals a lot about the quality of

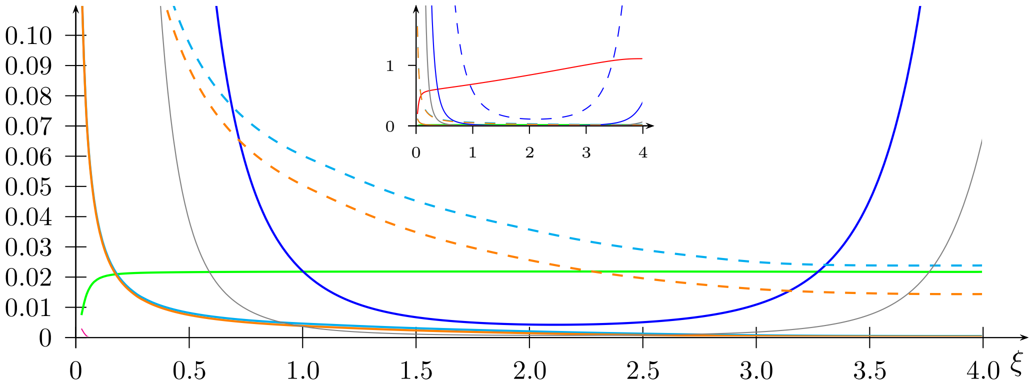


Figure 10.3: Errors of the various estimates relative to $\widetilde{\kappa}^k_{B,C}$. Parameters are as in Figure 10.1.

our estimates. The black area indicates the best that we could hope for, namely the estimate based merely on Prime number theorem 0.3. However, as this is difficult to evaluate we have to approximate once more. The λ estimate, shown in light gray, is clearly only of use to get a rough idea. The η estimate, however, is rather close to the actual behavior and may well serve as a basis for stochastic fine tuning of algorithms like the general number field sieve.

Last, Figure 10.3 illustrates the size of the various errors terms relative to $\widetilde{\kappa}^k$:

— $\widetilde{\lambda}$ error: $\left(1-\frac{1}{(1+\alpha)^k}\right)\widetilde{\lambda}^k(x)$.

— $\widetilde{\eta}$ error: $\left(1-\left(\frac{\ln(1+\alpha)}{\alpha}(1+\alpha)^{\frac{1}{\ln(1+\alpha)}-\frac{1}{\alpha}}\right)^k\right)\widetilde{\eta}^k(x)$.

— $\widehat{\lambda}$ error bound: $\widehat{c}_k\alpha^k x$. - - - Unconditional $\widehat{\lambda}$ error bound: $\widehat{c}_k\alpha^k x$.

— $\widehat{\lambda}$ error: $\widehat{\lambda}^k(x)$. - - - Unconditional $\widehat{\lambda}$ error: $\widehat{\lambda}^k(x)$.

— $\widehat{\kappa}$ error: $\widehat{\kappa}^k_{B,C}(x)$. - - - Unconditional $\widehat{\kappa}$ error: $\widehat{\kappa}^k_{B,C}(x)$.

— Non-squarefree error bound: $\left(2^{k-1}k!-s(k)\right)\frac{x}{B}$.

— Non-squarefree error: $\left(2^{k-1}k!-s(k)\right)\frac{x}{B}$.

For the unconditional errors we use Dusart's unconditional bound on $|\pi(x)-\mathrm{Li}(x)|$ which is given by $\widehat{E}(x)=2.3854\frac{x}{\ln^3 x}$ for $x \geq 355\,991$.

The figure shows that all the error terms but the $\widetilde{\lambda}$ error are sufficiently small. Our best choice is the $\widetilde{\eta}$ estimate which is ruled by the $\widetilde{\eta}$ error and the $\widehat{\lambda}$ error. Both are fairly less than 3% of the target value at least in the middle of the interval. The estimations are more difficult close to the boundaries. It is also positive that, at the parameters of our interest, most error terms are still comparative in size to the contributions of the $\widehat{\kappa}$ error, which is induced by the prime number theorem.

Definitely, the η estimate, combining the $\widetilde{\eta}$ error and the $\widehat{\lambda}$ error, is good enough for practical purposes, as for example the fine tuning of the general number field sieve.

Acknowledgements

This work was funded by the b-it foundation and the state of North Rhine-Westphalia. We thank Igor Shparlinski for his remarks.

References

ANDREAS DECKER & PIETER MOREE (2008). Counting RSA-integers. *Results in Mathematics* **52**, 35–39. URL `http://dx.doi.org/10.1007/s00025-008-0285-5`.

PIERRE DUSART (1998). *Autour de la fonction qui compte le nombre de nombres premiers.* Thèse de doctorat, Université de Limoges. URL `http://www.unilim.fr/laco/theses/1998/T1998_01.html`.

KEVIN FORD (2002a). Vinogradov's integral and bounds for the Riemann zeta function. *Proceedings of the London Mathematical Society (3)* **85**, 565–633. URL `http://dx.doi.org/10.1112/S0024611502013655`.

KEVIN FORD (2002b). Zero-free regions for the Riemann zeta function. In *Number Theory for the Millenium (Urbana, IL, 2000)*, M. A. BENNETT, BRUCE C. BERNDT, N. BOSTON, H. G. DIAMOND, ADOLF J. HILDEBRAND & W. PHILIPP, editors, volume II, 25–56. A. K. Peters. ISBN 978-1568811468. URL `http://www.math.uiuc.edu/~ford/wwwpapers/zeros.pdf`.

ANDREW GRANVILLE (2008). Smooth numbers: computational number theory and beyond. In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, JOSEPH P. BUHLER & PETER STEVENHAGEN, editors, number 44 in Mathematical Sciences Research Institute Publications, 69–82. Cambridge University Press, New York. ISBN 978-0-521-80854-5. URL `http://www.math.leidenuniv.nl/~psh/ANTproc/09andrew.pdf`.

NIELS FABIAN HELGE VON KOCH (1901). Sur la distribution des nombres premiers. *Acta Mathematica* **24**(1), 159–182. URL `http://dx.doi.org/10.1007/BF02403071`.

ANDREY V. KULSHA (2008). Values of $\pi(x)$ and $\Delta(x)$ for different x's. Webpage. URL `http://www.primefan.ru/stuff/primes/table.html`. Last visited 2 February 2009.

DANIEL LOEBENBERGER & MICHAEL NÜSKEN (2011). Analyzing standards for RSA integers — full version. *Submitted to Journal of Cryptology* URL `http://arxiv.org/abs/1104.4356`.

HERBERT ROBBINS (1955). A Remark on Stirling's Formula. *The American Mathematical Monthly* **62**(1), 26–29. URL `http://www.jstor.org/stable/2308012`.

JOHN BARKLEY ROSSER & LOWELL SCHOENFELD (1962). Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics* **6**, 64–94.

JOHN BARKLEY ROSSER & LOWELL SCHOENFELD (1975). Sharper Bounds for the Chebyshev Functions $\vartheta(x)$ and $\psi(x)$. *Mathematics of Computation* **29**(129), 243–269. URL `http://www.jstor.org/stable/2005479`.

LOWELL SCHOENFELD (1976). Sharper bounds for the Chebyshev functions $\vartheta(x)$ and $\psi(x)$. II. *Mathematics of Computation* **30**(134), 337–360.

TOMÁS OLIVEIRA E SILVA (2003). Fast implementation of the segmented sieve of Eratosthenes. WWW. URL `http://www.ieeta.pt/~tos/software/prime_sieve.html`. Simple implementation of the segmented sieve of Eratosthenes, released under the version 2 (or any later version) of the GNU general public license. Last visited 4 February 2009.

JACQUES CHARLES FRANÇOIS STURM (1835). Mémoire sur la résolution des équations numériques. *Mémoires présentés par divers savants à l'Acadèmie des Sciences de l'Institut de France* **6**, 273–318.

HERBERT SAUL WILF (1994). *generatingfunctionology*. Academic Press, 2nd edition. URL `http://www.math.upenn.edu/~wilf/DownldGF.html`. First edition 1990.

DANIEL LOEBENBERGER
b-it
Universität Bonn
Dahlmannstr. 2
D53012 Bonn
daniel@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/

MICHAEL NÜSKEN
b-it
Universität Bonn
Dahlmannstr. 2
D53012 Bonn
nuesken@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/