Revisiting the Random Subset Sum problem
Arthur Carvalho Walraven da Cunha, Francesco d’Amore, Frédéric Giroire,
Hicham Lesfari, Emanuele Natale, Laurent Viennot

To cite this version:
Arthur Carvalho Walraven da Cunha, Francesco d’Amore, Frédéric Giroire, Hicham Lesfari,
Emanuele Natale, et al.. Revisiting the Random Subset Sum problem. 31st Annual European
Symposium on Algorithms (ESA 2023), Sep 2023, Amsterdam, Netherlands. pp.37:1–37:11,
10.4230/LIPIcs.ESA.2023.37. hal-03654720v2

HAL Id: hal-03654720
https://hal.science/hal-03654720v2
Submitted on 30 Mar 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
Revisiting the Random Subset Sum Problem

Arthur C. W. Da Cunha1, Francesco D’Amore1,2, Frédéric Giroire1, Hicham Lesfari1,
Emanuele Natale1, and Laurent Viennot3

1Université Côte d’Azur, Inria Sophia Antipolis, CNRS
2Aalto University
3Inria Paris, IRIF

{arthur.carvalho-walraven-da-cunha,frederic.giroire,
hicham.lesfari,emanuele.natale,laurent.viennot}@inria.fr
francesco.damore@aalto.fi

Abstract

The average properties of the well-known Subset Sum Problem can be studied by the means of its randomised version, where we are given a target value \( z \), random variables \( X_1, \ldots, X_n \), and an error parameter \( \varepsilon > 0 \), and we seek a subset of the \( X_i \)'s whose sum approximates \( z \) up to error \( \varepsilon \). In this setup, it has been shown that, under mild assumptions on the distribution of the random variables, a sample of size \( O(\log(1/\varepsilon)) \) suffices to obtain, with high probability, approximations for all values in \( [-1/2, 1/2] \). Recently, this result has been rediscovered outside the algorithms community, enabling meaningful progress in other fields. In this work we present an alternative proof for this theorem, with a more direct approach and resourcing to more elementary tools.

1 Introduction

In the Subset Sum Problem (SSP), one is given as input a set of \( n \) integers \( X = \{x_1, x_2, \ldots, x_n\} \) and a target value \( z \), and wishes to decide if there exists a subset of \( X \) that sums to \( z \). That is, one is to reason about a subset \( S \subseteq [n] \) such that \( \sum_{i \in S} x_i = z \). The special case where \( z \) is half of the sum of \( X \) is known as the Number Partition Problem (NPP). The converse reduction is also rather immediate.

Be it in either of these forms, the SSP finds applications in a variety of fields, ranging from combinatorial number theory [Sun03] to cryptography [GJ01, KG11]. In complexity theory, the SSP is a well-known NP-complete problem, being a common base for NP-completeness proofs. In fact, the NPP version figures among Garey and Johnson’s six basic NP-hard problems [GJ79]. Under certain circumstances, the SSP can be challenging even for heuristics that perform well for many other NP-hard problems [JAMS91, RNMS96], and a variety of dedicated algorithms have been proposed to solve it [HM18, BW21, JW18, JVW21, EM19]. Nonetheless, it is not hard to solve it in polynomial time if we restrict the input integers to a fixed range [Bel66]. It suffices to recursively list all achievable sums using the first \( i \) integers: we start with \( A_0 = \{0\} \) and compute \( A_{i+1} = A_i \cup \{a + x_{i+1} \mid a \in A_i\} \). For integers in the range \([0, R]\), the search space has size \( O(nR) \).

1To find a subset of \( X \) summing to \( z \), one only needs to solve the NPP for the set \( X \cup \{2z, \sum_{i \in [n]} x_i\} \). By doing so, one of the parts must consist of the element \( \sum_{i \in [n]} x_i \) alongside the desired subset.
Studying how the problem becomes hard as we consider larger ranges of integers (relative to \( n \)) requires a randomised version of the problem, the Random Subset Sum Problem (RSSP), where the input values are taken as independently and identically distributed random variables. In this setup, the work \[BCP01\] proved that the problem experiences a phase transition in its average complexity as the range of integers increases.

The result we approach in this work comes from related studies on the typical properties of the problem. In \[Lue98\] the author proves that, under fairly general conditions, the expected minimal distance between a subset sum and the target value is exponentially small. More specifically, they show the following result.

**Theorem 1** (Lueker, 1998). Let \( X_1, \ldots, X_n \) be independent uniform random variables over \([-1,1]\), and let \( \varepsilon \in (0,1/3) \). There exists a universal constant \( C > 0 \) such that, if \( n \geq C \log(1/\varepsilon) \), then, with probability at least \( 1 - \varepsilon \), for all \( z \in [-1,1] \) there exists \( S_z \subseteq \{n\} \) for which

\[
|z - \sum_{i \in S_z} X_i| \leq \varepsilon.
\]

That is, a rather small number (of the order of \( \log \frac{1}{\varepsilon} \)) of random variables suffices to have a high probability of approximating not only a single target \( z \), but all values in an interval.

Even though Theorem \(\Box\) is stated and proved for uniform random variables over \([-1,1]\), it is not hard to extend the result to a wide class of distributions\(^2\). With this added generality, the theorem becomes a powerful tool for the analysis of random structures, and has recently proven to be particularly useful in the field of Machine Learning, taking part in a proof of the Strong Lottery Ticket Hypothesis \[PRN^{+20}\] and in subsequent related works \[dCNV22, FB21, BLMG22\], and in Federated Learning \[WDM^{+21}\].

Generalisations of the RSSP have played important roles in the study of random Knapsack problems \[BV03, BV04\], and to random binary integer programs \[BDHT22, BDHK22\]. In particular, the works \[BdCC^{+22}, BDHK22, BDHT22\] recently provided an extension of Theorem \(\Box\) to multiple dimensions. As for the equivalent Random Number Partitioning Problem, \[CJRS22\] recently generalised \[BCP01\] and the integer version of the RSSP to non-binary integer coefficients.

The simplicity and ubiquity of the SSP has granted the related results a special didactic place. Be it as a first example of NP-complete problem \[GJ79\], a path to science communication \[Hay02\], or simply as a frame for the demonstration of advanced techniques \[Mer01\], it has been a tool to make important, but sometimes complicated, ideas easier to communicate.

This work offers a substantially simpler alternative to the original proof of Theorem \(\Box\) by following a general framework introduced in the context of the analysis of Rumour Spreading algorithms \[DK17\]. Originally, the work \[Lue98\] approaches Theorem \(\Box\) by considering the random variable associated to the proportion of the values in the interval \([-1,1]\) that can be approximated up to error \( \varepsilon \) by the sum of some subset of the first \( t \) variables, \( X_1, \ldots, X_t \).

After restricting to some specific types of subsets, they proceed to evaluate the expected per-round growth of this proportion, conditioned on the outcomes of \( X_1, \ldots, X_t \). Their strategy is to analyse this expected increase by martingale theory, which only becomes possible after a non-linear transformation of the variables of interest. Those operations hinder any intuition for the obtained martingale. Nonetheless, a subsequent application of the Azuma-Hoeffding bound \[Azu67\] followed by a case analysis leads to the result.

\(^2\)Distributions whose probability density function \( f \) satisfies \( f(x) \geq b \) for all \( x \in [-a, a] \), for some constants \( a, b > 0 \) (see Corollary 3.3 from \[Lue98\]).
The argument presented here starts in the same direction as the original one, tracking the mass of values with suitable approximations as we reveal the values of the random variables \(X_1, \ldots, X_n\) one by one. However, we quickly diverge from [Lue98], managing to obtain an estimation of the expected growth of this mass without discarding any subset-sum. We eventually restrict the argument to some types of subsets, but we do so at a point where the need for such restriction is clear.

We proceed to directly analyse the estimation obtained, without any transformations. Following [DK17], this estimation reveals two expected behaviours in expectation, which can be analysed in a similar way: as we consider the first variables, the proportion of approximated values grows very fast; then, after a certain point, the proportion of non-approximable values decreases very fast.

We remark that, while Theorem \(\Box\) crucially relies on tools from martingale theory such as Azuma-Hoeffding’s inequality, which are not part of standard Computer Science curricula, our argument makes use of much more elementary results which should make it accessible enough for an undergraduate course on randomised algorithms.

2 Our argument

In this section, we provide an alternative argument for proving Theorem \(\Box\). It takes shape much like the pseudo-polynomial algorithm we described in the introduction. Leveraging the recursive nature of the problem, we construct a process which, at time \(t\), describes the proportion of the interval \([-1, 1]\) that can be approximated by some subset of the first \(t\) variables.

We will show that with a suitable number of uniform variables (proportional to \(\log(1/\varepsilon)\)) a factor of \(1 - \varepsilon/2\) of the values in \([-1, 1]\) can be approximated up to error \(\varepsilon\). This implies that any \(z \in [-1, 1]\) which cannot be approximated within error \(\varepsilon\) is at most \(\varepsilon\) away from a value that can. Therefore it is possible to approximate \(z\) up to error \(2\varepsilon\).

2.1 Preliminaries

Let \(X_1, \ldots, X_n\) be realisations of random variables as in Theorem \(\Box\) and, without loss of generality, fix \(\varepsilon > 0\). We say a value \(z \in \mathbb{R}\) is \(\varepsilon\)-approximated at time \(t\) if and only if there exists \(S \subseteq [t]\) such that \(|z - \sum_{i \in S} X_i| < \varepsilon\). For \(0 \leq t \leq n\), let \(f_t : \mathbb{R} \to \{0, 1\}\) be the indicator function for the event “\(z\) is \(\varepsilon\)-approximated at time \(t\)”. Therefore, we have \(f_0 = \mathbb{1}_{(-\varepsilon, \varepsilon)}\), since only the interval \((-\varepsilon, \varepsilon)\) can be approximated by an empty set of values. From there, we can exploit the recurrent nature of the problem: a value \(z\) can be \(\varepsilon\)-approximated at time \(t + 1\) if and only if either \(z\) or \(z - X_{t+1}\) could already be approximated at time \(t\). This implies that for all \(z \in \mathbb{R}\) we have that

\[
f_{t+1}(z) = f_t(z) + (1 - f_t(z)) f_t(z - X_{t+1}).
\]

To keep track of the proportion of values in \([-1, 1]\) that can be \(\varepsilon\)-approximated at each step, we define, for each \(0 \leq t \leq n\), the random variable

\[
v_t = \frac{1}{2} \int_{-1}^{1} f_t(z) \, dz.
\]

For better readability, throughout the text we will refer to \(v_t\) simply as “the volume.”

As we mentioned, it suffices to show that, with high probability, at time \(n\), enough of the interval is \(\varepsilon\)-approximated (more precisely, that \(v_n \geq 1 - \varepsilon/2\)) to conclude that the entire interval is \(2\varepsilon\)-approximated.

\[4\text{Namely, the intermediate value theorem, Markov’s inequality, and standard Hoeffding bounds.}\]
2.1.1 Expected behaviour

Our first lemma provides a lower bound on the expected value of $v_t$.

**Lemma 1.** For all $0 \leq t < n$, it holds that

$$E[v_{t+1} \mid X_1, \ldots, X_t] \geq v_t \left[ 1 + \frac{1}{4} (1 - v_t) \right].$$

**Proof.** The definition of $v_t$ and the recurrence in Eq. (1) give us that

$$E[v_{t+1} \mid X_1, \ldots, X_t] = E \left[ \frac{1}{2} \int_{-1}^{1} f_{t+1}(z) \, dz \mid X_1, \ldots, X_t \right]$$

$$= \int_{-1}^{1} \frac{1}{2} \left( \frac{1}{2} \int_{-1}^{1} f_t(z) + (1 - f_t(z)) f_t(z - x) \, dz \right) \, dx$$

$$= \frac{1}{2} \int_{-1}^{1} f_t(z) \, dz \int_{-1}^{1} \frac{1}{2} \, dx + \frac{1}{2} \int_{-1}^{1} \frac{1}{2} \int_{-1}^{1} (1 - f_t(z)) f_t(z - x) \, dz \, dx$$

$$= v_t + \frac{1}{4} \int_{-1}^{1} (1 - f_t(z)) \int_{-1}^{1} f_t(z - x) \, dx \, dz$$

$$= v_t + \frac{1}{4} \int_{-1}^{1} (1 - f_t(z)) \int_{z-1}^{z+1} f_t(y) \, dy \, dz,$$

where the last equality holds by substituting $y = z - x$. For the previous ones we apply basic properties of integrals and Fubini’s theorem to change the order of integration.

We now look for a lower bound for the last integral in terms of $v_t$. To this end, we exploit that, since all integrands are non-negative, for all $u \in [-1/2, 1/2]$ we have that

$$\int_{-1}^{1} (1 - f_t(z)) \int_{z-1}^{z+1} f_t(y) \, dy \, dz \geq \int_{u-1/2}^{u+1/2} (1 - f_t(z)) \int_{z-1}^{z+1} f_t(y) \, dy \, dz$$

$$\geq \int_{u-1/2}^{u+1/2} (1 - f_t(z)) \int_{u-1/2}^{u+1/2} f_t(y) \, dy \, dz.$$
 Altogether, we can conclude that
\[
\mathbb{E}[v_{t+1} \mid X_1, \ldots, X_t] = v_t + \frac{1}{4} \int_{-1}^{1} (1 - f_t(z)) \int_{z-\frac{X_{t+1}}{2}}^{z+\frac{X_{t+1}}{2}} f_t(y) \, dy \, dz \\
\geq v_t + \frac{1}{2} \int_{u^* - \frac{X_{t+1}}{2}}^{u^* + \frac{X_{t+1}}{2}} (1 - f_t(z)) \left( \frac{1}{2} \int_{u^* - \frac{X_{t+1}}{2}}^{u^* + \frac{X_{t+1}}{2}} f_t(y) \, dy \right) \, dz \\
= v_t + \left( \frac{1}{2} - \frac{v_t}{2} \right) \frac{v_t}{2} \\
= v_t \left[ 1 + \frac{1}{4} (1 - v_t) \right].
\]

Lemma 1 tells us that, if \( v_t \) were to behave as expected, it should grow exponentially up to \( 1/2 \), at which point \( 1 - v_t \) starts to decrease exponentially. The rest of the proof follows accordingly, with Section 2.2 analysing the progress of \( v_t \) up to one half, and Section 2.3 analogously following the complementary value, \( 1 - v_t \), starting from one half. By building on the results from Section 2.2, we obtain fairly straightforward proofs in Section 2.3. Thus, the following subsection comprises the core of our argument.

2.2 Growth of the volume up to 1/2

Arguably, the main challenge in analysing the RSSP is the existence of over-time dependencies and deciding how to overcome it sets much of the course the proof will take. Our strategy consists in constructing another process which dominates the original one while being free of dependencies.

Let \( \tau_1 \) be the first time at which the volume exceeds \( 1/2 \), that is, let
\[
\tau_1 = \min\{t \geq 0 : v_t > 1/2\}.
\]

We just proved that up to time \( \tau_1 \) the process \( v_t \) enjoys exponential growth in expectation. In the following lemma we apply a basic concentration inequality to translate this property into a constant probability of exponential growth for \( v_t \) itself.

**Lemma 2.** Given \( \beta \in (0, 1/8) \), let \( p_\beta = 1 - \frac{7}{8(1-\beta)} \). For all integers \( 0 \leq t < \tau_1 \) it holds that
\[
\Pr\left[ v_{t+1} \geq v_t (1 + \beta) \mid X_1, \ldots, X_t, t < \tau_1 \right] \geq p_\beta.
\]

**Proof.** The result shall follow easily from reverse Markov's inequality [BGPS06, Lemma 4] and the bound from Lemma 1. However, doing so requires a suitable upper bound on \( v_{t+1} \) and, while \( 2v_t \) would serve the purpose, such bound does not hold in general.

We overcome this limitation by fixing \( t \) and considering how much \( v_t \) would grow in the next step if we were to consider only values \( \varepsilon \)-approximated at time \( t \) that happen to lie in \([-1, 1]\) after being translated by \( X_{t+1} \). Making it precise by the means of the recurrence in Eq. (1), we define
\[
\tilde{v} = \frac{1}{2} \int_{-1}^{1} \left[ f_t(z) + (1 - f_t(z)) f_t(z - X_{t+1}) \cdot 1_{[-1,1]}(z - X_{t+1}) \right] \, dz.
\]

This expression differs from the one for \( v_{t+1} \) only by the inclusion of the characteristic function of \([-1, 1]\). This not only implies that \( \tilde{v} \leq v_{t+1} \), but also that \( \tilde{v} \) can replace \( v_{t+1} \) in the bound from Lemma 1 since the argument provided there eventually restricts itself to integrals within \([-1, 1]\),
trivialising $I_{[-1,1]}$. Moreover, as we obtain $\tilde{v}$ without the influence of values from outside $[-1,1]$, we must have $\tilde{v} \leq 2v_t$. Finally, using that $t < \tau_1$ implies $v_t < 1/2$ and chaining the previous conclusions in respective order, we conclude that
\[
\Pr \left[ v_{t+1} \geq v_t(1 + \beta) \mid X_1, \ldots, X_t, t < \tau_1 \right] \geq \Pr \left[ \tilde{v} \geq v_t(1 + \beta) \mid X_1, \ldots, X_t, t < \tau_1 \right] \\
\geq \frac{\mathbb{E}[\tilde{v} \mid X_1, \ldots, X_t, t < \tau_1] - v_t(1 + \beta)}{2v_t - v_t(1 + \beta)} \\
\geq \frac{\frac{9}{8}v_t - v_t(1 + \beta)}{2v_t - v_t(1 + \beta)} \\
= 1 - \frac{7}{8(1 - \beta)},
\]
where we applied the reverse Markov’s inequality in the second step.

The previous lemma naturally leads us to look for bounds on $\tau_1$, that is, to estimate the time needed for the process to reach volume $1/2$. As expected, the exponential nature of the process yields a logarithmic bound.

**Lemma 3.** Let $t$ be an integer and given $\beta \in (0, 1/8)$, let $p_\beta = 1 - \frac{7}{8(1 - \beta)}$ and $i^* = \left\lceil \log \frac{1}{2} \log(1 + \beta) \right\rceil$.

If $t \geq i^*/p_\beta$, then
\[
\Pr \left[ \tau_1 \leq t \right] \geq 1 - \exp \left[ -\frac{2p_\beta}{t} \left( t - \frac{i^*}{p_\beta} \right)^2 \right].
\]

**Proof.** The main idea behind the proof is to define a new random variable which stochastically dominates $\tau_1$ while being simpler to analyse. We begin by discretising the domain $(0, 1/2]$ of the volume into sub-intervals $\{I_i\}_{0 \leq i \leq i^*}$ defined as follows:
\[
\begin{align*}
I_0 &= (0, \varepsilon), \\
I_i &= (\varepsilon(1 + \beta)^{i-1}, \varepsilon(1 + \beta)^i) \text{ for } 1 \leq i < i^*, \\
I_{i^*} &= (\varepsilon(1 + \beta)^{i^*-1}, 1/2],
\end{align*}
\]
where $i^*$ is the smallest integer for which $\varepsilon(1 + \beta)^{i^*} \geq 1/2$, that is, $i^* = \left\lceil \log \frac{1}{2} \log(1 + \beta) \right\rceil$.

Now, for each $i \geq 0$, we direct our interest to the number of steps required for $v_t$ to exit the sub-interval $I_i$ after first entering it. By Lemma 2, this number is majorised by a geometric random variable $Y_i \sim \text{Geom}(p_\beta)$. Therefore, we can conclude that $\tau_1$ is stochastically dominated by the sum of such variables, that is, for $t \in \mathbb{N}$, we have that
\[
\Pr \left[ \tau_1 \geq t \right] \leq \Pr \left[ \sum_{i=1}^{i^*} Y_i \geq t \right].
\]

Let $B_t \sim \text{Bin}(t, p_\beta)$ be a binomial random variable. For the sum of geometric random variables, it holds that $\Pr \left[ \sum_{i=1}^{i^*} Y_i \leq t \right] = \Pr \left[ B_t \geq i^* \right]$. Since $\mathbb{E}[B_t] = tp_\beta$, the Hoeffding bound for binomial
random variables \cite[Theorem 1.1]{DP09} implies that, for all $\lambda \geq 0$, we have that $\Pr[B_t \leq tp_\beta - \lambda] \leq \exp(-2\lambda^2/t)$. Setting $t$ such that $tp_\beta - \lambda = i^*$, we obtain that

$$\Pr\left[ \sum_{i=1}^{i^*} Y_i \geq t \right] \leq \Pr[B_t \leq i^*] \leq \exp\left[ -\frac{2}{t} \left( tp_\beta - i^* \right)^2 \right] = \exp\left[ -\frac{2p_\beta^2}{t} \left( t - \frac{i^*}{p_\beta} \right)^2 \right],$$

which holds as long as $\lambda = tp_\beta - i^* \geq 0$, that is, for all $t \geq \frac{1}{p_\beta} \left[ \log \frac{1}{2} \epsilon \log(1+ \beta) \right]$.

The thesis follows by applying this to Eq. (2) and passing to complementary events.

### 2.3 Growth of the volume from $1/2$

Here we study the second half of the process: from the moment the volume reaches $1/2$ up to the time it gets to $1 - \epsilon/2$. We do so by analysing the complementary stochastic process, i.e., by tracking, from time $\tau_1$ onwards, the proportion of the interval $[-1, 1]$ that does not admit an $\epsilon$-approximation. More precisely, we consider the process $\{w_t\}_{t \geq 0}$, defined by $w_t = 1 - v_{\tau_1 + t}$.

We shall obtain results for $w_t$ similar to those we have proved for $v_t$. Fortunately, building on the previous results makes those proofs quite straightforward. We start by noting that a statement analogous to Lemma 1 follows immediately from the definition of $w_{t+1}$ and Lemma 1.

**Corollary 4.** For all $t \geq 0$, it holds that

$$\mathbb{E}[w_{t+1} | X_1, \ldots, X_{\tau_1 + t}] \leq w_t \left[ 1 - \frac{1}{4} (1 - w_t) \right].$$

Let $\tau_2$ the first time that $w_t$ gets smaller than or equal to $\epsilon/2$, that is, let

$$\tau_2 = \min \{ t \geq 0 : w_t \leq \epsilon/2 \}.$$

The following lemma bounds this quantity, in analogy to Lemma 3.

**Lemma 5.** For all $t > 0$, it holds that

$$\Pr[\tau_2 \leq t] \geq 1 - \frac{1}{\epsilon} \left( \frac{7}{8} \right)^t.$$

**Proof.** Applying that $1 - w_t = v_{\tau_1 + t} > 1/2$ to Lemma 4 gives the bound

$$\mathbb{E}[w_{t+1} | X_1, \ldots, X_{\tau_1 + t}] \leq \frac{7}{8} w_t. \tag{3}$$

Moreover, from the conditional expectation theory, for any two random variables $X$ and $Y$, we have $\mathbb{E}[\mathbb{E}[X | Y]] = \mathbb{E}[X]$. From this and Eq. (3), we can conclude that

$$\mathbb{E}[w_t] = \mathbb{E}\left[ \mathbb{E}[w_t | X_1, \ldots, X_{\tau_1 + t-1}] \right] \leq \frac{7}{8} \mathbb{E}[w_{t-1}],$$

which, by recursion, yields that

$$\mathbb{E}[w_t] \leq \left( \frac{7}{8} \right)^t \mathbb{E}[w_0] \leq \frac{1}{2} \left( \frac{7}{8} \right)^t.$$

Finally, by Markov’s inequality,

$$\Pr[\tau_2 \geq t] \leq \Pr(w_t \geq \frac{\epsilon}{2}) \leq \frac{2 \mathbb{E}[w_t]}{\epsilon} \leq \frac{1}{\epsilon} \left( \frac{7}{8} \right)^t,$$

and the thesis follows from considering the complementary event. \qed
2.4 Putting everything together

In this section we conclude our argument, finally proving Theorem 1. We first prove a more general statement and then detail how it implies the theorem.

Let $\tau = \tau_1 + \tau_2$, the first time at which the process $\{v_t\}_{t\geq 0}$ reaches at least $1 - \varepsilon/2$.

**Lemma 6.** Let $\varepsilon \in (0, 1/3)$. There exist constants $C' > 0$ and $\kappa > 0$ such that for every $t \geq C' \log \frac{1}{\varepsilon}$, it holds that

$$\Pr[\tau \leq t] \geq 1 - 2 \exp \left[ -\frac{1}{\kappa t} \left( t - C' \log \frac{1}{\varepsilon} \right)^2 \right].$$

**Proof.** Let $\beta = \frac{1}{16}$ and $p_\beta = 1 - \frac{7}{8(1-\beta)} = \frac{1}{15}$. The definition of $\tau$ allows us to apply Lemmas 3 and 4 quite directly. Indeed, if, for the sake of Lemma 3, we assume

$$t \geq \frac{2}{p_\beta} \left[ \frac{\log \frac{1}{\varepsilon}}{\log(1+\beta)} \right],$$

we have that

$$\Pr[\tau \leq t] = \Pr[\tau_1 + \tau_2 \leq t] \geq \Pr[\tau_1 \leq t/2, \tau_2 \leq t/2] \geq \Pr[\tau_1 \leq t/2] + \Pr[\tau_2 \leq t/2] - 1 \geq 1 - \exp \left[ -\frac{p_\beta^2}{t} \left( t - 2 \frac{1}{p_\beta} \left[ \frac{\log \frac{1}{\varepsilon}}{\log(1+\beta)} \right] \right)^2 \right] - \frac{1}{\varepsilon} \left( \frac{7}{8} \right)^{t/2} = 1 - \exp \left[ -\frac{1}{15^2 t} \left( t - 30 \left[ \frac{\log \frac{1}{\varepsilon}}{\log \frac{17}{16}} \right] \right)^2 \right] - \frac{1}{\varepsilon} \left( \frac{7}{8} \right)^{t/2},$$

where the second inequality holds by the union bound. The remaining of the proof consists in computations to connect this expression to the one in the statement.

Consider the first exponential term in Eq. (4). Taking $t \geq \frac{60 \log \frac{17}{16} \cdot \log \frac{1}{\varepsilon}}{\varepsilon}$, since $\varepsilon < 1/3$, it follows that

$$\exp \left[ -\frac{1}{15^2 t} \left( t - 30 \left[ \frac{\log \frac{1}{\varepsilon}}{\log \frac{17}{16}} \right] \right)^2 \right] \leq \exp \left[ -\frac{1}{15^2 t} \left( t - 60 \frac{\log \frac{1}{\varepsilon}}{\log \frac{17}{16}} \cdot \log \frac{1}{\varepsilon} \right)^2 \right].$$

Now, consider the second exponential term in Eq. (4). It holds that

$$\frac{1}{\varepsilon} \left( \frac{7}{8} \right)^{t/2} = \exp \left[ \log \frac{1}{\varepsilon} - \frac{t}{2} \log \frac{8}{7} \right] \leq \exp \left[ \log \frac{1}{\varepsilon} - \frac{t}{15} \right] = \exp \left[ -\frac{1}{15} \cdot \frac{1}{t - 15 \cdot \log \frac{1}{\varepsilon}} \cdot \left( t - 15 \cdot \log \frac{1}{\varepsilon} \right)^2 \right].$$

Moreover, for $t \geq 15 \cdot \log \frac{1}{\varepsilon}$,

$$\exp \left[ -\frac{1}{15} \cdot \frac{1}{t - 15 \cdot \log \frac{1}{\varepsilon}} \cdot \left( t - 15 \cdot \log \frac{1}{\varepsilon} \right)^2 \right] \leq \exp \left[ -\frac{1}{15t} \left( t - 15 \cdot \log \frac{1}{\varepsilon} \right)^2 \right] \leq \exp \left[ -\frac{1}{15^2 t} \left( t - \frac{60 \log \frac{17}{16} \cdot \log \frac{1}{\varepsilon}}{\varepsilon} \right)^2 \right].$$
Altogether, we have that
\[
\exp \left[ -\frac{p^2}{t} \left( t - \frac{2}{p} \log \left( \frac{\log \left( \frac{1}{2} \right)}{\log(1 + \beta)} \right) \right) \right] + \frac{1}{\varepsilon} \cdot \left( \frac{7}{8} \right)^{t/2} \leq 2 \exp \left[ -\frac{1}{15^2} \left( t - \frac{60}{\log(\frac{17}{16})} \log \left( \frac{1}{\varepsilon} \right) \right) \right],
\]
and the thesis follows by setting \( \kappa = 15^2 \) and \( C' = 60/\log(17/16) \).

The expression in the claim of Lemma 6 can be reformulated as
\[
\Pr \left[ v_t \geq 1 - \frac{\varepsilon}{2} \right] \geq 1 - 2 \exp \left[ -\frac{1}{\kappa t} \left( t - C' \log \left( \frac{1}{\varepsilon} \right) \right)^2 \right];
\]
hence, Theorem 1 follows by taking \( C \geq 3C' \) and observing that once we can approximate all but an \( \varepsilon/2 \) proportion of the interval \([-1, 1]\), any \( z \in [-1, 1] \) either is \( \varepsilon \)-approximated itself, or is at most \( \varepsilon \) away from a value that is, which implies that \( z \) is \( 2\varepsilon \)-approximated.

References


