Contention Resolution, With and Without a Global Clock*

Zixi Cai
IIIS, Tsinghua University

Kuowen Chen
IIIS, Tsinghua University

Shengquan Du
IIIS, Tsinghua University

Tsvi Kopelowitz
Bar-Ilan University

Seth Pettie
University of Michigan

Ben Plosk
Bar-Ilan University

Abstract

In the Contention Resolution problem n parties each wish to have exclusive use of a shared resource for one unit of time. A canonical example is n devices that each must broadcast a packet of information on a shared channel, but the same principles apply to other distributed systems. The problem has been studied since the early 1970s, under a variety of assumptions on feedback (collision detection, etc.) given to the parties, how the parties wake up (synchronized, adversarial, random), knowledge of n, and so on. The most consistent assumption is that parties do not have access to a *global clock*, only their *local time* since wake-up. This is surprising because the assumption of a global clock is both technologically realistic and algorithmically interesting. It enriches the problem, and opens the door to entirely new techniques.

In this paper we introduce the *GlobalClock* model and establish several new complexity separations, both between GlobalClock and the usual LocalClock model, and within the LocalClock model. Our primary results are:

GlobalClock vs. LocalClock. We design a new Contention Resolution protocol that guarantees latency $O\left(\left(n \log\log n \log^{(3)} n \log^{(4)} n \cdots \log^{(\log^* n)} n\right) \cdot 2^{\log^* n}\right) \le n(\log\log n)^{1+o(1)}$ in expectation and with high probability. This already establishes at least a roughly-$\log n$ complexity gap between randomized protocols in GlobalClock and LocalClock.

In-Expectation vs. With-High-Probability. Prior analyses of randomized Contention Resolution protocols in LocalClock guaranteed a certain latency *with high probability*, i.e., with probability $1 - 1/\operatorname{poly}(n)$. We observe that it is just as natural to measure *expected latency*, and prove a $\log n$-factor complexity gap between the two objectives for memoryless protocols. The In-Expectation complexity is $\Theta(n \log n / \log\log n)$ whereas the With-High-Probability latency is $\Theta(n \log^2 n / \log\log n)$. Three of these four upper and lower bounds are new.

No Universally Optimal Protocols. Given the complexity separation above, one would naturally want a Contention Resolution protocol that is optimal under *both* the In-Expectation and With-High-Probability metrics. This is impossible! It is even impossible to achieve In-Expectation latency $o(n \log^2 n/(\log\log n)^2)$ and With-High-Probability latency $n \log^{O(1)} n$ simultaneously.

*This work was conducted while the first three authors were visiting University of Michigan. Supported by NSF Grant CCF-2221980.

1 Introduction

In the abstract *Contention Resolution* problem there are n parties, where n is typically unknown, which are interested in monopolizing some shared resource for one unit of time. In each time step, the only actions the parties can take are to *idle* or *grab* the shared resource. If exactly one party attempts to grab the shared resource, it succeeds in monopolizing it for that unit of time, but if two or more try to grab it, they all fail. The premier application of abstract Contention Resolution is to facilitate n devices to access a shared communications channel, who each want to transmit a packet of information. This application may allow for explicit coordination between the parties, e.g., if they are allowed to transmit extra information (beyond their packets), which can be received by other parties. The umbrella of Contention Resolution captures dozens of distinct algorithm design problems, depending on the modeling assumptions and metrics of efficiency. Let us highlight the key choices that must be made in fixing a model.

Wake-Up times. The parties may be woken up synchronously [BFG06], or at times chosen by an adversary, or via a statistical process, typically a Poisson point process [Gal78, Cap79, MT81, MH85]. In this paper we assume adversarial wake-up times.

Feedback. It is always assumed that every party that attempts to grab the shared resource immediately perceives whether it is successful or not. Protocols for which this is the *only* feedback are called *acknowledgment based*. In general, the system may provide ternary $\{0, 1, 2+\}$-feedback (aka *collision detection*) [Gal78, Cap79, MT81, MH85, GFL87, BKPY18, CJP19] to all parties indicating that zero, one, or at least two parties attempted to grab the resource, or binary $\{0/2+, 1\}$-feedback [AMM13, BKKP20, DKS22a] indicating only failure or success.[1] We work exclusively with acknowledgment-based protocols.

Deterministic vs. Randomized. When parties have unique IDs in the range $[N]$, $n \leq N$, it is possible to solve Contention Resolution deterministically, in time that depends on n and N. See [KG85, Kha89, CMS01, CGKR05, DK15] and the references therein. In contrast, instantiations of randomized algorithms are identical, and break symmetry via locally flipping coins. Following most work in the area, this paper assumes identical randomized parties.

Finite vs. Unbounded. In the $\{0, 1, 2+\}$- and $\{0/2+, 1\}$-feedback models, there exist protocols [BFGY19, CJP19, BKKP20] that run infinitely, without deadlock. In this setting *throughput* is the main measure of efficiency.[2] Acknowledgment-based protocols are typically analyzed under the assumption that n is finite, and usually unknown, where the main metric is *latency* as a function of n. This is the gap between a party's wake-up time and the time it monopolizes the shared resource. Our results only consider the finite setting.

Adversarial Power. If the wake-up times of the parties are chosen by an adversary, one can still distinguish between an *oblivious adversary*, which chooses n and all wake-up times at the beginning, and an *adaptive adversary*, which decides how many parties to wake up in each time step based on the state and history of all parties. Our results hold under the weakest assumption: an adaptive adversary when proving upper bounds, and an oblivious adversary when proving lower bounds.

[1] In the context of a shared communication channel, some protocols assume that $O(\log n)$ bits can be transmitted in the case of success (i.e., "1"); see [BKPY18].

[2] I.e., the maximum long-term rate of new party wake-ups that can be sustained in such a way that the *backlog* is bounded, infinitely often.

This list captures only a subset of models from the literature, and leaves out recent work on *resilient* protocols [BFGY19, CJP19, BFG+24], that work even against an adversary that can "jam" the shared channel, as well as *energy efficient* protocols [BKPY18, BFG+24], that are awake (receive feedback $\{0, 1, 2+\}$ or $\{0/2+, 1\}$) for a small number of time slots.

Maximally Efficient Protocols. Perhaps the most important take-away message from prior work is that protocols achieving *constant throughput* in the unbounded setting or *linear latency* in the finite setting are only known to be possible in a few situations:

- Constant throughput/linear latency is possible under a Poisson or adversarial wake-up schedule, as long as $\{0, 1, 2+\}$- or $\{0/2+, 1\}$-feedback is given [Cap79, MH85, TM78, MT81, BFGY19, BKPY18, BKKP20, CJP19, BFG+24, DKS22a, GFL87].
- If the n parties (n unknown) wake up synchronously, $O(n)$ latency is possible w.h.p. via the *sawtooth* protocol of Bender et al. [BFH+04], which is acknowledgment-based.
- If the n parties agree on an approximation $N = \Theta(n)$, then $O(n)$ latency is possible via the acknowledgment-based protocol of De Marco and Stachowiak [DS17], even under adversarial wake-up times.

Because acknowledgment-based protocols are limited in their ability to perceive contention, they seem to be incapable of achieving constant throughput (unbounded) or linear latency (finite) in general. De Marco and Stachowiak [DS17] proved this in the finite setting, specifically that against an oblivious adversary, the maximum latency of some party is $\Omega(n \log n / \log^2 \log n)$ with high probability. In the unbounded setting, Goldberg and Lapinskas [GL25] proved that outside of a tiny class of "LCED" protocols,[3] all memoryless[4] acknowledgment-based protocols are *unstable* under Poisson arrivals, for any rate $\lambda > 0$. I.e., with probability 1 the throughput eventually goes to 0 and the backlog of unsuccessful parties goes to ∞. In light of these results, we ask the natural question:

Question 1.1. What are the *minimal additional assumptions* necessary to allow a randomized acknowledgment-based protocol to achieve linear latency in the finite setting, or constant throughput in the unbounded setting?

One contribution of this paper is to explore a natural assumption that *could* satisfy Question 1.1.

Global Clocks. Nearly all prior work assumes that each party only perceives their own *local time* since wake-up. To our knowledge, the assumption of a *global clock* known to all parties has never been seriously explored in the usual randomized setting, though De Marco and Kowalski [DK15] did make this assumption in designing a *deterministic* protocol, where the parties have unique IDs in $[N]$. This is quite strange, since such an assumption is both technologically realistic and intellectually interesting. Assuming the *GlobalClock* model does not trivialize the (randomized) Contention Resolution problem, but it does open up the *design-space* of Contention Resolution protocols. The first two questions to ask about this model are naturally: *is GlobalClock strictly more powerful than the standard LocalClock model?* and *is the GlobalClock assumption an answer to Question 1.1?* Specifically, is latency $O(n)$ possible?

[3] LCED: *largely constant with exponential decay*

[4] AKA *backoff*-type protocols, meaning the behavior of a party depends on its clock, not its past actions.

1.1 New Results

In this paper we work exclusively with randomized, acknowledgment-based protocols, and consider protocols in both the LocalClock and GlobalClock models. Recall that *acknowledgment-based* means the parties receive *no feedback* except at the moment of their own success. All of our algorithms are *memoryless*, meaning their behavior depends only on the clocks (local or local and global), not on the history of their behavior, and our lower bounds apply to memoryless algorithms. (Golberg and Lapinskas call these *backoff-type* algorithms; Bender et al. [BFH+05] call them *Bernoulli* algorithms.)

The GlobalClock Model. We give the *first* randomized Contention Resolution protocol that exploits the GlobalClock model.

Theorem 1.1. *There is an acknowledgment-based Contention Resolution protocol in the GlobalClock model that achieves latency* $O(n\zeta(4\log\log n)) = n(\log\log n)^{1+o(1)}$ *with high probability, where*

$$\zeta(x) = (2x)(2\log x)(2\log^{(2)} x)\cdots(2\log^{(\log^* x)} x).$$

The peculiar ζ function is derived from Elias's ω-code [Eli75] for the integers. Theorem 1.1 and the lower bound of De Marco, Kowalski, and Stachowiak [DKS22b] establish a complexity separation between GlobalClock and LocalClock.

Corollary 1.2. *GlobalClock is* strictly *more powerful than LocalClock, in the sense that acknowledgment-based Contention Resolution protocols can have latency* $n(\log\log n)^{1+o(1)}$ *in the former (Theorem 1.1), but must have latency* $\Omega(n\log n/(\log\log n)^2)$ *in the latter [DS17, DKS22b], with high probability.*

We believe that Theorem 1.1 just scratches the surface in terms of new techniques, and that *linear latency* may be within reach. Conjecture 1.3 lays out what we think should be possible in this model.

Conjecture 1.3. *Consider the class of randomized acknowledgment-based protocols in the GlobalClock model.*

1. *In the finite setting, there exists a protocol with latency* $O(n)$ *with high probability against an adaptive adversary.*
2. *In the unbounded setting, there exists a stable protocol assuming a Poisson wake-up process, for some rate* $\lambda > 0$.
3. *In the unbounded setting, there exists a protocol that utilizes the shared resource at some rate* λ,[5] *even against an adaptive adversary.*

Due to the non-adversarial nature of Conjecture 1.3(2), it should be considered the most plausible. Conjecture 1.3(3) is the least plausible, and should only be attacked once Conjecture 1.3(1) is first established.

[5]Here we have in mind the definition of utilization implicit in the analysis of [CJP19]. Utilization λ is achieved if (1) there is a potential function Φ such that waking up n' parties increases Φ by at most n'/λ, (2) if $\Phi = \Omega(1)$ is sufficiently large, executing the protocol for another time step decreases Φ by $1+\epsilon$ in expectation, $\epsilon > 0$, and (3) if $\Phi = O(1)$ is bounded, the number of still-unsuccessful parties left in the system is also $O(1)$. This definition does not constrain the adversary, e.g., by limiting the wake-up rate to λ over certain windows of time [BFH+05].

The LocalClock Model. Prior work in the traditional LocalClock model proved that a certain latency L is achieved *with high probability* [BFH+05, DS17, DKS22b]. It is just as natural to seek protocols that guarantee a certain latency *in expectation*. We establish asymptotically sharp bounds on the latency of memoryless protocols under both metrics, which reveals a complexity separation between these two objective functions. Three of the four bounds of Theorem 1.4 are new.

Theorem 1.4 (In-Expectation vs. With-High-Probability)**.** *Consider the class of memoryless, acknowledgment-based LocalClock protocols.*

1. *There exists a protocol with latency $O(n \log^2 n / \log\log n)$* ***with high probability****, even aginst an adaptive adversary. See De Marco, Kowalski, and Stachowiak [DS17, DKS22b] and Section 6.*
2. *There exists a protocol with latency $O(n \log n / \log\log n)$* ***in expectation****, even against an adaptive adversary. See Section 6.*
3. *No protocol has latency $o(n \log^2 n / \log\log n)$* ***with high probability****, even against an oblivious adversary.*[6] *See Section 5.*
4. *No protocol has latency $o(n \log n / \log\log n)$* ***in expectation****, even against an oblivious adversary. See Section 5.*

Given the complexity separation between **In-Expectation** and **With-High-Probability** metrics, the natural followup question is: can we at least run *one* protocol that is optimal under *both* metrics? In most models of computation the answer would obviously be *yes*: just run two optimal protocols in parallel/interleaved. There is no such generic interleaving method in the LocalClock model, and in fact it is *impossible* to simultaneously achieve optimality under both metrics. Theorem 1.5 shows something even stronger, that there is essentially no interesting trade-off possible between **In-Expectation** and **With-High-Probability** guarantees.

Theorem 1.5. *No acknowledgment-based memoryless Contention Resolution protocol in the LocalClock model can simultaneously guarantee both $o(n \log^2 n / \log^2 \log n)$ latency in expectation and $n \log^{O(1)} n$ latency with high probability.*

1.2 Organization

In Section 2 we give a brief technical overview of the paper, focussing mainly on the lower bounds of Theorem 1.4(3,4) and Theorem 1.5. In Section 3 we formally define the LocalClock and GlobalClock models, protocols in those models, the latency metrics, and useful notation used throughout the paper. In Section 4 we give the first randomized Contention Resolution algorithm in the GlobalClock model. Section 5 presents the $\Omega(n \log n / \log\log n)$ and $\Omega(n \log^2 n / \log\log n)$ lower bounds of Theorem 1.4(3,4) in the LocalClock model, and Section 6 presents matching upper bounds, including an alternate proof of the $O(n \log^2 n / \log\log n)$ upper bound from [DS17, DKS22b]. We conclude with some open problems in Section 7.

[6] Is saying g cannot be $o(f)$ the same as saying $g = \Omega(f)$? It depends on who you ask. See Appendix A.

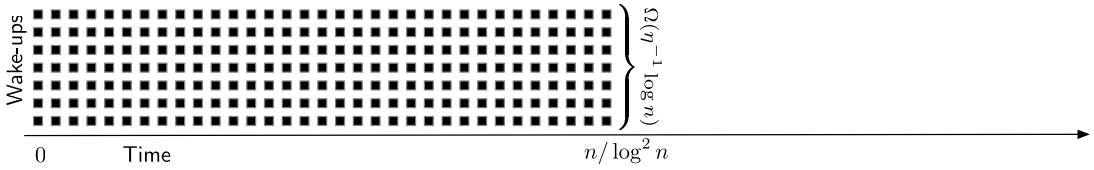
2 Technical Overview

At any particular time step t, the *contention* σ is the sum, over all active parties u, that u attempts to grab the shared resource. The probability of *some* party being successful is roughly $\sigma e^{-\sigma}$ so for a protocol to be efficient it must create many constant-contention slots. Conversely, in a lower bound, the adversary typically tries to sustain $\omega(1)$ contention over a long period of time.

GlobalClock Protocol. The problem with binary exponential backoff or any similar protocol is that it is easy for the (oblivious) adversary to maintain contention $\omega(1)$ over a long period of time. In Section 4 we exploit the fact that parties have access to a common global clock t by interpreting a suffix of the bits in the binary representation of t as an integer $a(t)$, and using $a(t)$ to *synchronize* a multiplicative modification to the default grab-probability of binary exponential backoff. At any particular time we do not know the best integer ℓ, so we let $(a(t))$ cycle through *all* integers according to a certain schedule determined by Elias's γ-code [Eli75], in which integer ℓ appears periodically with period at most $(2\ell)(2\log\ell)(2\log\log\ell)(2\log\log\log\ell)\cdots(2\log^{(\log^*\ell)}\ell)$.

LocalClock Upper Bounds. It is sometimes difficult to prove upper bounds against adaptive adversaries because the *strategy space* of the adversary is so large. The main innovation in Section 6 is to reduce the analysis of contention resolution protocols to what we call a *counter game*, whose optimal strategy is obvious. By fixing the optimal strategy, counter games can be analyzed in a straightforward fashion with standard Chernoff bounds.

LocalClock Lower Bounds. Section 5 is the most technically involved. We build on the lower bound technique of De Marco, Kowalski, and Stachowiak [DS17, DKS22b], in which we progressively build up an adversary in *layers*. Layers 0 and 1 are from [DS17, DKS22b]. For this overview we consider the *latency with high probability* metric.

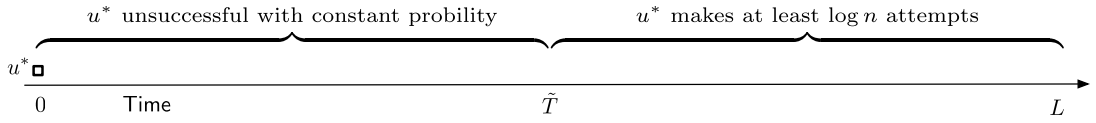


Layer 0. Each party, without loss of generality, attempts to grab the resource at local time 1 with constant probability, say η. Thus, by waking up $\Theta(\eta^{-1}\log n)$ parties per time step for $\Theta(n/\log^2 n)$ time steps we ensure zero successes in this interval, w.h.p., while waking up a negligible fraction of the parties.

Layer 1. A most important quantity of a protocol is $s(x)$: the expected number of times a party attempts to grab the resource in its first x times slots. Identify some party u^* woken up at time zero, and let $L = L(n) < n\,\mathrm{polylog}(n)$ be its latency deadline. We wake up the remaining $n - o(n)$

parties at random times in $[1, L]$. Every time u^* attempts to grab the shared resource in the interval $[n/\log^2 n, L]$, it collides with a newly awoken party, with probability $1/\operatorname{polylog}(n)$. Thus, to achieve success with high probability it must be that $s(L) - s(n/\log^2 n) = \Omega(\log n/\log\log n)$. We can of course find an n' for which $L(n') = n/\log^2 n$ and conclude that $s(L(n')) - s(n'/\log^2 n') = \Omega(\log n'/\log\log n')$, and so on. We know that $L(n) < n\operatorname{polylog}(n)$ so by a telescoping sum calculation, $s(n) = \Omega((\log n/\log\log n)^2)$. Thus—ignoring the effect of successes—the average contention over $[0, L]$ is roughly $\Omega(ns(L)/L)$. Setting $L = \Theta(n\log n/(\log\log n)^2)$ maintains contention $\Omega(\log n)$ over $[0, L]$, ensuring that there are, in fact, no successful parties with high probability.

Layer 2. Guaranteeing *no* successes in the interval $[0, L]$ is stronger than necessary when lower bounding the latency L. Suppose we set $L = \Theta(n\log^2 n/(\log\log n)^3)$, so the average contention becomes $\Theta(ns(L)/L) = \Omega(\log\log n)$. However, now each time step sees a success with probability $1/\operatorname{polylog}(n)$, and as the successful party exits the system it *reduces* the contention of future time steps, thereby *increasing* the probability of success in the future, and so on. We show that this feedback loop does not spin out of control, and that the contention remains $\Omega(\log\log n)$ over the interval $[0, L]$. By itself this argument would lead to an $\Omega(n\log^2 n/(\log\log n)^3)$ lower bound. However, our ambition is to prove a *sharp* $\Omega(n\log^2 n/\log\log n)$ lower bound, matching the asymptotic complexity of [DS17, DKS22b].



Layer 3. Define $\tilde{T}$ to be such that an adversary that wakes up a constant fraction of the n parties can prevent a party u^* released at time zero from achieving success by time $\tilde{T}$, with constant probability. We establish two bounds capturing the dependence between s and $\tilde{T}$, which are informally stated below in a *highly simplified* form.

$$\tilde{T} \geq \frac{ns(n)}{\log\log n}, \tag{1}$$

$$s(L) - s(\tilde{T}) \geq \log n. \tag{2}$$

These bounds have a *circular* relationship, in the sense that a weak lower bound on $s(\cdot)$ implies a lower bound on $\tilde{T}$ via Equation (1), which then implies an stronger lower bound on $s(\cdot)$ via Equation (2). This cycling converges on a fixed point of $s(n) = \Omega(\log^2 n)$ and $L \geq \tilde{T} = \Omega(n\log^2 n/\log\log n)$. (The actual statements corresponding to Equations (1) and (2) are significantly more complicated than written above, but this discussion captures the flavor of the proof.)

Under different parameterization the same sequence of layers leads to an $\Omega(n\log n/\log\log n)$ lower bound on expected latency, and the impossibility of simultaneous optimality along the In-Expectation and With-High-Probability metrics.

3 Models, Metrics, and Basic Protocols

Timing and Clocks. Time is partitioned into discrete slots indexed by $\mathbb{N}$. There are n identical parties, which we index by $[n]$ for notational convenience. Let $t_u \in [n]$ be the wake-up time of party u. In the GlobalClock model, at time t, u perceives both t and its local time $t - t_u$, whereas in the LocalClock model, it only perceives $t - t_u$.

Strategy Space. A *protocol* in the LocalClock model is a distribution $\mathcal{D}$ over $\{0,1\}^*$, under the interpretation that if $X^{(u)} = (X_1^{(u)}, X_2^{(u)}, \ldots) \sim \mathcal{D}$, then party u will attempt to grab the shared resource at local time t_{loc} iff $X_{t_{\mathsf{loc}}}^{(u)} = 1$ and u did not achieve success before local time t_{loc}. A protocol in the GlobalClock model is a family of distributions $\mathcal{D} = (\mathcal{D}_{t^*})_{t^* \in \mathbb{N}}$ over $\{0,1\}^*$, where t^* represents the global wake-up time of the party. In other words, if $X^{(u)} = (X_1^{(u)}, X_2^{(u)}, \ldots) \sim \mathcal{D}_{t_u}$, then u attempts to grab the shared resource at global time $t_u + t_{\mathsf{loc}}$ iff $X_{t_{\mathsf{loc}}}^{(u)} = 1$ and u has yet to achieve success before this time.

A protocol is called *memoryless* if $\Pr(X_{t_{\mathsf{loc}}}^{(u)} = 1)$ depends only on the clocks ($t_{\mathsf{loc}} = t - t_u$ or both t, t_{loc}) and not the prior history of party u, i.e., $X_1^{(u)}, \ldots, X_{t_{\mathsf{loc}}-1}^{(u)}$. We often identify a memoryless protocol $\mathcal{D}$ in the LocalClock model by the function $p(i) \stackrel{\text{def}}{=} \Pr\left[X_i^{(u)} = 1\right]$, where $\mathcal{D}$ is normally omitted.

Active Sets and the Adversary. Let $\hat{A}[t]$ be the set of all parties woken up by time t, and let $A[t \mid t_0] \subseteq \hat{A}[t]$ be those parties woken up by time t and yet to achieve success by time t_0. $A[t]$ is short for $A[t \mid t]$. The number of parties woken up at each time step is decided by an adversarial strategy $\mathcal{A}$. Let $\mathcal{A}[n]$ be the adversary that is constrained to wake up n parties.

Latency. Let t_u^{succ} be the time when u first achieves success, i.e., $X_{t_u^{\text{succ}} - t_u}^{(u)} = \sum_{v \in A[t_u^{\text{succ}}]} X_{t_u^{\text{succ}} - t_v}^{(v)} = 1$. Define $L_{\mathcal{D},\mathcal{A}[n]}^{(u)} = t_u^{\text{succ}} - t_u$ to be the *latency* of u, which is a random variable whose distribution depends on n, the protocol $\mathcal{D}$, and adversarial strategy $\mathcal{A}[n]$. Minimizing latency is the objective, but there are two natural ways to look at this metric:

- **Expected Latency.** The goal is to choose $\mathcal{D}$ to minimize the growth of the function

$$L_{\mathcal{D}}^{\text{exp}}(n) = \sup_{\mathcal{A}[n]} \max_{u \in [n]} \mathbb{E}\left[L_{\mathcal{D},\mathcal{A}[n]}^{(u)}\right].$$

  In other words, every party should enjoy a bound on its own expected latency, as a function of n.

- **Latency With High Probability.** Given a failure probability threshold $q = q(n)$, the goal is to choose $\mathcal{D}$ to minimize the latency bound $L_{\mathcal{D}}(n, q)$, which satisfies

$$\forall \mathcal{A}[n].\ \forall u \in [n].\ \Pr\left[L_{\mathcal{D},\mathcal{A}[n]}^{(u)} \leq L_{\mathcal{D}}(n,q)\right] \geq 1 - q.$$

  We define $L_{\mathcal{D}}^{\text{whp}}(n) = L_{\mathcal{D}}(n, n^{-2})$, where the error threshold n^{-2} is arbitrary. Note that $L_{\mathcal{D}}(n, 1/2) \leq 2L_{\mathcal{D}}^{\text{exp}}(n)$ by Markov's inequality.

Perhaps the most notorious Contention Resolution protocol is *Binary Exponential Backoff* (BEB). Upon waking up at time t_u, u partitions all future time slots in *windows* $(t_u, t_u + 1], (t_u + 1, t_u + 2], \ldots, (t_u + 2^i, t_u + 2^{i+1}], \ldots$ and attempts to grab the shared resource at a uniformly random time slot in each window. Observe that the probability that BEB grabs the resource at time $t_u + t_{\mathsf{loc}}$ is $\Theta(1/t_{\mathsf{loc}})$. Thus, BEB is sometimes expressed as a *memoryless* protocol with $p(t_{\mathsf{loc}}) = \Pr\left[X_{t_{\mathsf{loc}}}^u = 1\right] = \Theta(1/t_{\mathsf{loc}})$, independent of u's history. The simplicity of BEB is attractive, but it is theoretically undesirable under many metrics. For example, in the unbounded setting it deadlocks

with probability 1 when parties are woken up according to a Poisson point process with *any* constant rate [Ald87, GL25]. Even if all parties are synchronized, its latency is only $O(n \log n)$ with high probability, rather than optimal $O(n)$ [BFH+05].

The following notation are used in the analysis of LocalClock algorithms and lower bounds.

Aggregate Contention—Static. Recall that for a memoryless protocol $\mathcal{D}$, $p(t_{\mathsf{loc}}) = p_{\mathcal{D}}(t_{\mathsf{loc}}) \stackrel{\text{def}}{=} \Pr\left[X_{t_{\mathsf{loc}}}^{(u)} = 1\right]$ is the probability of any party u grabbing the resource at local time t_{loc}. For a global time slot t and a set of parties S, define

$$\hat{\sigma}[t; S] = \hat{\sigma}_{\mathcal{A},\mathcal{D}}[t; S] \stackrel{\text{def}}{=} \sum_{u \in S} p(t - t_u)$$

to be the *static aggregate contention* contributed by S at time t, with respect to a fixed protocol $\mathcal{D}$ and oblivious adversary $\mathcal{A}$. For brevity, we write $\hat{\sigma}[t] = \hat{\sigma}[t; \hat{A}[t]]$. We emphasize that S is a *fixed* set chosen before the execution, making $\hat{\sigma}[t; S]$ static in nature: it is not dependent on the randomness of the parties.

History Prior to Global Time t We denote by H_t the *history prior to global time t*, that is, the collection of all observations made by all parties before time t. In particular, it includes the information $(X_\tau^{(u)})_{1 \le \tau < t - t_u}$ for all $u \in \hat{A}[t]$. We say that a set of parties S is *H_t-measurable* if it is a function of H_t.

Aggregate Contention—Dynamic. When $S = S(H_t)$ is H_t-measurable, we use different notation to measure *dynamic aggregate contention*. Define

$$\sigma[t; S(H_t)] \stackrel{\text{def}}{=} \sum_{u \in S(H_t)} p(t - t_u).$$

For brevity $\sigma[t] = \sigma[t; A[t]]$. Sometimes we may write $\sigma[t; S(H_{t_0})]$ to emphasize that S only depends on the history up until time $t_0 \le t$. It need not be the case that $S \subset A[t]$; it is also useful to measure the aggregate contention that *would* have been contributed by parties $S \subset \hat{A}[t] \backslash A[t]$ who already achieved success before time t.

Sum of Access Probabilities. For a memoryless protocol $\mathcal{D}$, define the function $s = s_{\mathcal{D}}$ as

$$s(k) = \sum_{t_{\mathsf{loc}}=1}^{k} p(t_{\mathsf{loc}}) = \mathbb{E}\left[\sum_{t_{\mathsf{loc}}=1}^{k} X_{t_{\mathsf{loc}}}^{(u)}\right], \qquad \text{which does not depend on } u.$$

That is, $s(k)$ is the expected number of attempts at the shared resource in the first k steps, where the subscript may be dropped if implicit.

The following lemma is standard in analyzing Contention Resolution protocols. The probability of success is maximized when the sum of probabilities of parties grabbing the shared resource is constant. See Appendix C.1 for proof.

Lemma 3.1. *For a global time t, let $p_u = \Pr\left[X^{(u)}_{t-t_u} = 1\right]$ be the probability that u grabs the shared resource and $\sigma = \sigma[t] = \sum_{u \in A[t]} p_u$.*

1. *If $p_u \in [0, 1/2]$ for all $u \in A[t]$, then $\Pr\left[\left(\sum_{u \in A[t]} X^{(u)}_{t-t_u}\right) = 1\right] \geq \sigma 4^{-\sigma}$, and u's probability of success is at least $p_u 4^{-\sigma}$.*
2. $\Pr\left[\left(\sum_{u \in A[t]} X^{(u)}_{t-t_u}\right) = 1\right] \leq \sigma e^{-\sigma+1}$ *and* $\Pr\left[\left(\sum_{u \in A[t]} X^{(u)}_{t-t_u}\right) \leq 1\right] \leq e^{-\sigma} + \sigma e^{-\sigma+1}$.

4 Contention Resolution with a Global Clock

Our memoryless algorithm makes use of *Elias codes*, which we now review. For a positive integer, let $\texttt{Bin}(N) \in \{\texttt{0}, \texttt{1}\}^*$ be the $(1 + \lfloor \log_2 N \rfloor)$-bit binary representation of N. Define the sequence $N = N_1, N_2, \ldots, N_k = 1$ where $N_i = \lfloor \log_2 N_{i-1} \rfloor$. Elias's ω-code [Eli75] assigns a bit-string $\texttt{Code}(N)$ to each positive integer N:

$$\texttt{Code}(N) = \texttt{Bin}(N_{k-1})\,\texttt{Bin}(N_{k-2}) \cdots \texttt{Bin}(N_1)\,\texttt{0}.$$

For example, $\texttt{Code}(1) = \texttt{0}$, $\texttt{Code}(2) = \texttt{10 0}$, $\texttt{Code}(3) = \texttt{11 0}$, $\texttt{Code}(4) = \texttt{10 100 0}$, with spaces introduced for clarity.

Lemma 4.1. *The set $\{\texttt{Code}(N)\}_{N \in \mathbb{Z}^+}$ is a prefix-free code and the length of $\texttt{Code}(N)$ is $1 + (1 + \lfloor \log N \rfloor) + (1 + \lfloor \log \lfloor \log N \rfloor \rfloor) + \cdots + (2)$.*

We define an infinite sequence $(a(t))_{t \in \mathbb{N}}$ of positive integers indexed by the global time t as follows. Let $S = \texttt{Bin}(t)^R\texttt{000}\cdots$ be an infinite bit-string obtained by reversing the binary representation of t, then padding it with an infinite suffix of 0s. Let $\texttt{Code}(N) = S[0]S[1]\cdots S[|\texttt{Code}(N)| - 1]$ be the prefix of S in the code book, and set $a(t) = N$. We will also require an infinite sequence $(a'(t))$ over $\mathbb{Z}$. Define

$$a'(t) = (-1)^{a(t) \bmod 2} \lfloor a(t)/2 \rfloor .$$

Recall from the introduction that $\zeta(x) = (2x)(2\log x)(2\log^{(2)} x)\cdots(2\log^{(\log^* x)} x)$.

Lemma 4.2. *The sequences $(a(t))_{t \in \mathbb{N}}$ and $(a'(t))_{t \in \mathbb{N}}$ have the following properties.*

1. *Let k be a positive integer and $I \subset \mathbb{N}$ be any interval of width $2^{|\texttt{Code}(k)|} \leq \zeta(k)$. Then $\{1, 2, \ldots, k\}$ is a subset of $\{a(t) \mid t \in I\}$.*
2. *Let k be a positive integer and $I \subset \mathbb{N}$ be an interval of width $2^{|\texttt{Code}(2k+1)|} \leq \zeta(2k+1)$. Then $\{0, \pm 1, \pm 2, \ldots, \pm(k-1), \pm k\}$ is a subset of $\{a'(t) \mid t \in I\}$.*

Proof. The first claim follows from the fact that k appears in $(a(t))$ periodically with period $2^{|\texttt{Code}(k)|} \leq \zeta(k)$, and that for positive $k' < k$, $|\texttt{Code}(k')| \leq |\texttt{Code}(k)|$. The second claim follows from the fact that $\{1, \ldots, 2k+1\}$ are mapped onto $\{0, \pm 1, \pm 2, \ldots, \pm(k-1), \pm k\}$. □

4.1 The Algorithm

The memoryless version of BEB grabs the shared resource with probability $1/(t-t_u)$, i.e., inversely proportional to u's time since wake-up. Define $\tau(t) = \sum_{u \in A[t]} 1/(t-t_u)$ to be the "natural" BEB contention at time t. If all parties knew $\alpha = 1/\tau(t)$, they could grab with probability $\alpha/(t-t_u)$, leading to a constant success probability, by Lemma 3.1. Using the global clock, Algorithm 1 uses $a'(t)$ to synchronize guesses to $\log \alpha$. The code is written from the perspective of an arbitrary party u. Until u is successful, the variable t_u^{succ} should be treated as ∞.

Algorithm 1: $\mathsf{ContRes}(t, t_u)$: t is global time, t_u is u's wake-up time, t_u^{succ} is success time.

```
1 if t ∈ [t_u, t_u^succ)                    // u is awake, but not yet successful
2 then
3 |  u grabs the resource with probability min{ 1/2, 2^{a'(t)} / (t − t_u) }.
4 end
```

Observe that Algorithm 1 can only be executed in the GlobalClock model as it uses t to synchronize the behavior of the parties.

Lemma 4.3. *Let $\tau(t) = \sum_{u \in A[t]} \frac{1}{t-t_u}$ and $k = \lceil |\log \tau(t)| \rceil$. Absent new wake-ups, Algorithm 1 has a constant probability of seeing at least one success in the interval $[t, t + \zeta(2k+1)]$.*

Proof. By Lemma 4.2, within the interval $[t, t+2^{|\mathsf{Code}(2k+1)|}) \subseteq [t, t+\zeta(2k+1)]$ there are times t_1, t_2 such that $a'(t_1) = k, a'(t_2) = -k$. (Notice that $\log \tau(t)$ can be either positive or negative.) Absent any new wake-ups, and assuming no successes took place in any time slot $t' \notin \{t_1, t_2\}$, Lemma 3.1 implies that Algorithm 1 has a constant probability of success in time slot t_1 or t_2. □

Corollary 4.4. *If $\tau(t) \in [\frac{1}{8c} \log^{-2} n, 8c \log^2 n]$ then in the time interval*

$$[t, t + \zeta\left(2\lceil 2 \log\log n + \log 8c \rceil + 1\right)] = [t, t + (\log\log n)^{1+o(1)}),$$

absent new wake-ups, Algorithm 1 has a constant probability of seeing at least one success.

Let $\lambda = \lceil 2 \log\log n + \log 8c \rceil$ for some constant $c \geq 1$ controlling the probability of error. In the analysis, we partition time into *blocks* with width $\zeta(2\lambda+1) = (\log\log n)^{1+o(1)}$.

Corollary 4.4 says that whenever $\tau(t) \in [\frac{1}{8c \log^2 n}, 8c \log^2 n]$, we have a constant probability of success in the next block, absent new wake-ups. Define a block to be *heavy* or *light*, respectively, if the block is free of new wake-ups and $\tau(t) > 8c \log^2 n$, or $\tau(t) < \frac{1}{8c \log^2 n}$. A block that is neither heavy nor light and free of new wake-ups is called a *normal* block.

Lemma 4.5. *Consider an n-party execution of Algorithm 1 during an interval $[t_0, t_0 + W]$ of width W. Then the number of heavy blocks during this interval is $O(\frac{n \log W}{\log^2 n})$.*

Proof. Consider the sum of $\tau(t)$ over the interval.

$$\sum_{t \in [t_0, t_0+W]} \tau(t) \leq \sum_{u \in [n]} \sum_{t=\max(t_0, t_u+1)}^{t_0+W} \frac{1}{t-t_u} \leq \sum_{u \in [n]} O(\log W) = O(n \log W).$$

Thus, there are at most $O(\frac{n \log W}{\log^2 n})$ time slots t with $\tau(t) > 8c \log^2 n$. □

Lemma 4.6. *Suppose party u is active at time t, where t is in some light block B and satisfies $a'(t) = \lceil 2 \log\log n + \log 4c \rceil$. Then, the probability that u successfully transmits at time t is at least $\frac{2c \log^2 n}{t - t_u}$.*

Proof. At time t, every active party v transmits with probability $p_v = \frac{2^{a'(t)}}{t - t_v}$. Specifically $p_u = \frac{2^{a'(t)}}{t - t_u} > \frac{4c \log^2 n}{t - t_u}$. Since B is a light block, $\tau(t) < \frac{1}{8c \log^2 n}$ and so $\hat{\sigma}[t] < \frac{2^{a'(t)}}{8c \log^2 n} < 1/2$, which implies that all parties in $A[t]$ transmit with probability at most $1/2$. By Lemma 3.1, u succeeds with probability at least $p_u 4^{-1/2} \geq \frac{2c \log^2 n}{t - t_u}$. □

Lemma 4.7. *There are at most $O(n)$ normal blocks with high probability.*

Proof. Consider a normal block B_i beginning at time t, $\tau(t) \in [\frac{1}{8c \log^2 n}, 8c \log^2 n]$ so Corollary 4.4 implies that there exists some constant $p_i = \Theta(1)$ such that the probability of success in the block is p_i. Let $p_{\min} = \min\{p_i\}$ be the minimum constant success probability across all normal blocks. By the Chernoff-Hoeffding bound (Appendix B), the probability that there are at least $\frac{2n}{p_{\min}}$ normal blocks is $\exp(-\Omega(n))$. □

Theorem 4.8. *Algorithm 1 has latency at most $L = O(n\zeta(4 \log\log n + O(1))) = n(\log\log n)^{1+o(1)}$, with high probability.*

Proof. For any party u, we prove that the latency of u is at most $L = \gamma n \zeta(2\lambda+1) = \gamma n \zeta(2\lceil 2 \log\log n + \log 8c \rceil + 1)$ with high probability, where γ is a constant determined later.

Consider the interval $(t_u, t_u + L]$. Recall that there are 4 types of blocks.

- **Blocks with new wake-ups:** There are at most n blocks that contain new wake-ups.
- **Heavy blocks:** By applying Lemma 4.5 to the interval $(t_u, t_u + L]$ of length L, there are at most $O(\frac{n \log L}{\log^2 n}) = o(n)$ heavy blocks.
- **Normal blocks:** By Lemma 4.7 there are at most $O(n)$ normal blocks throughout the execution of the algorithm, with high probability.
- **Light blocks:** The remaining blocks are all light blocks. Since $L = \gamma n \zeta(2\lambda + 1)$, we have $\frac{L}{\zeta(2\lambda+1)} = \gamma n$. Thus, the number of light blocks is at least $\frac{1}{2} \frac{L}{\zeta(2\lambda+1)}$ when γ is sufficiently large.

By Lemma 4.6, in every light block in which u is active, there exists a time slot t in which u succeeds with probability at least $\frac{2c \log^2 n}{t - t_u} \geq \frac{2c \log^2 n}{L}$. Thus, the probability that party u did not succeed during all the light blocks in which u is active is at most

$$\left(1 - \frac{2c \log^2 n}{L}\right)^{\frac{L}{2\zeta(2\lambda+1)}} \leq e^{-\frac{c \log^2 n}{\zeta(2\lambda+1)}} \leq e^{-c \log n} \leq \frac{1}{n^c}.$$

□

A note on non-linear approximations of n. De Marco and Stachowiak [DS17] proved that if the parties share a common approximation $N = \Theta(n)$, then linear latency can be achieved, even in the LocalClock model. Theorem 4.8 shows that in the GlobalClock model latency $O(n(\log\log n)^{1+o(1)})$ can be achieved, without any *a priori* knowledge of n.

We can modify Algorithm 1 to achieve latency $O(n \log\log N)$, where $N > n$ is an upper bound common to all parties. In other words, we can achieve latency $O(n \log\log n)$ even with any quasipolynomial approximation $N < 2^{\log^{O(1)} n}$. Rather than use the $(a'(t))$ sequence, we modify Algorithm 1 to grab with probability $2^k/(t-t_u)$, where k cycles through $\{-2\log\log N, \ldots, 2\log\log N\}$ periodically. The analysis of Theorem 4.8 still holds, substituting $(2\log\log N + 1)$ for $\zeta(2\lambda+1) = (\log\log n)^{1+o(1)}$.

5 Lower Bounds in the LocalClock Model

In this section, we establish the following lower bound for memoryless protocols.

Theorem 5.1 (Formal Statement of Theorem 1.4(3,4))**.** *There is no acknowledgment-based memoryless Contention Resolution protocol $\mathcal{D}$ that satisfies either*

With-High-Probability Guarantee $L_{\mathcal{D}}^{\text{whp}}(n) = o(n \log^2 n/\log\log n)$*, or*

In-Expectation Guarantee $L_{\mathcal{D}}^{\text{exp}}(n) = o(n \log n/\log\log n)$.

In the course of proving this theorem, we also obtain the following tradeoff showing that even *near*-optimal expected latency and *near*-optimal high-probability latency cannot be achieved at the same time.

Theorem 5.2 (Formal statement of Theorem 1.5)**.** *For any acknowledgment-based memoryless Contention Resolution protocol $\mathcal{D}$, $L_{\mathcal{D}}^{\text{exp}}(n) = o(\frac{n\log^2 n}{(\log\log n)^2})$ and $L_{\mathcal{D}}^{\text{whp}}(n) = n\log^{O(1)} n$ cannot be achieved simultaneously.*

Since the proofs in this section only involve oblivious adversaries, without loss of generality we may assume the protocol satisfies $\eta \stackrel{\text{def}}{=} p(1) > 0$. Before proceeding, we review two key definitions:

- $s(k) = \sum_{i=1}^{k} p(i)$ denotes the total attempt probability of a party in its local time $[1, k]$, which also equals the expected number of attempts made in this interval.
- $L_{\mathcal{D}}(n, q)$ is the latency bound such that, for each party, its actual latency is at most $L_{\mathcal{D}}(n, q)$ with probability at least $1 - q$. Throughout this section, $q = q(n)$ is either $q(n) = 1/2$ or $q(n) = n^{-2}$ depending on whether we are minimizing expected latency or latency with high probability.

De Marco, Kowalski, and Stachowiak [DKS22b] proved that there *does not exist* any acknowledgment-based protocol $\mathcal{D}$ for which

$$L_{\mathcal{D}}^{\text{whp}}(n) = o\left(\frac{n\log n}{(\log\log n)^2}\right).$$

In the following, we informally outline the key steps of their argument in our notation.

Structural overview of the De Marco, Kowalski, and Stachowiak lower bound [DKS22b].

- For any protocol $\mathcal{D}$, they constructed an adversary $\mathcal{A}$ that ensures $\hat{\sigma}_{\mathcal{A},\mathcal{D}}[t] = \Omega(\log n)$ for all $t \in [1, \Omega(n/\log^2 n)]$. In this case, the probability of success is $n^{-\Omega(1)}$ in $[1, \Omega(n/\log^2 n)]$.
- Focus on a specific party u^* that is activated at time 0. Since there is no success w.h.p in $[1, \Omega(n/\log^2 n)]$, u^* must make a sufficiently large number of attempts in the remaining time slots to guarantee success with latency $L_{\mathcal{D}}(n, n^{-2})$. It implies $s(L_{\mathcal{D}}(n, n^{-2})) - s(\Omega(n/\log^2 n)) \geq \Omega(\log n/\log\log n)$.
- Suppose $L_{\mathcal{D}}(n, n^{-2}) = O(n \operatorname{polylog}(n))$, so if we let $n' < n$ be such that $L(n') = n/\log^2 n$, then $n' = n/\operatorname{polylog}(n)$, and by the same argument above, $s(L(n')) - s(\Omega(n'/\log^2 n')) = \Omega(\log n'/\log\log n')$, and so on. By a telescoping-sum argument, $s(n) = \Omega\left(\frac{\log^2 n}{(\log\log n)^2}\right)$. Based on this result, they construct an adversary $\mathcal{A}'$ such that $\hat{\sigma}_{\mathcal{A}',\mathcal{D}}[t] = \Omega(\log n)$ for all $t \leq \Omega(n \cdot s(n)/\log n) = \Omega(n \log n/(\log\log n)^2)$. Hence, with high probability, there is no success in the first $\Omega(n \log n/(\log\log n)^2)$ time slots.

Key intuitive observations. For memoryless protocols, we refine the previous lower-bound framework by making the following two observations:

- The bottleneck in prior arguments is the requirement that $\hat{\sigma}[t] = \Omega(\log n)$ to guarantee *no success* with high probability. In contrast, our adversary maintains a weaker condition (approximately $\hat{\sigma}[t] = \Omega(\log\log n)$, though there are additional constraints), which permits $o(n)$ of the parties to succeed. The difficulty here is showing that the (dynamic) aggregate contention $\sigma[t]$ remains $\Omega(\log\log n)$ as well, as successful parties effectively remove aggregate contention from the system. This part of the analysis is enabled by a new tool of *probability thresholds* and *filtering*, which we discuss shortly. If only these ideas were applied, we would end up with a lower bound of $L^{\text{whp}}_{\mathcal{D}}(n) = \Omega(n \log^2 n/(\log\log n)^3)$.
- Our lower bound on $s(n) = \Omega(\log^2 n/(\log\log n)^2)$ turns out to be loose by a $(\log\log n)^2$ factor for bounding $L^{\text{whp}}_{\mathcal{D}}(n)$. In order to close this $(\log\log n)$-factor gap we need a more refined analysis. We define $\tilde{T}_{\mathcal{D}}(n)$ to be such that, with constant probability, we can keep one particular party from achieving success in $\tilde{T}$ time slots by waking up a constant fraction of the parties. We can simultaneously lower bound $\tilde{T}$ in terms of s, and lower bound $s(L^{\text{whp}}_{\mathcal{D}}(n)) - s(\tilde{T})$ by $\Omega(\log n)$ rather than $\Omega(\log n/\log\log n)$. Analyzing these two lower bounds in tandem ultimately lets us shave off the last two $\log\log n$ factors and achieve a sharp lower bound.

Overview and organization. The rest of this section is organized as follows:

- In Section 5.1, we introduce a family of thresholds $B_\beta(i) = \Theta(\log^\beta i/i)$ for a fixed constant β and for all $i \geq 1$. Most known protocols are smooth and monotonically decreasing. For example, the Binary Exponential Backoff (BEB) protocol corresponds to a memoryless protocol with $p(i) = \Theta(1/i)$, whereas the high-probability protocols of [DS17, DKS22b] use $p(i) = \Theta(\log i/i)$. In general, a *high-probability slot* (i.e., one with $p(i) > B_\beta(i)$) tends to have an undesirable effect on the analysis. Therefore, we introduce a filter function to exclude time slots whose transmission probabilities are excessively large, so that we can better capture the essential behavior of the protocol.

- Following the above argument, we explore the properties of probability thresholds. Throughout this section, we mainly focus on the following two functions:
  - $s^{\text{low}_\beta}(k) = \sum_{1 \le i \le k} p^{\text{low}_\beta}(i)$, where $p^{\text{low}_\beta}(i) = p(i) \cdot \mathbf{1}\{p(i) \le B_\beta(i)\}$ for $i \ge 1$. $s^{\text{low}_\beta}(k)$ represents the prefix sum of low probabilities.
  - To estimate the lower bounds, we identify one arbitrary party u^*, which is activated at time 0, and we focus on maximizing the latency of u^*. For these reasons, we introduce $\tilde{T}_{\mathcal{D}}(n)$ which represents the maximum number of time slots such that an adversary can use at most a constant fraction of the n parties to ensure that u^* cannot succeed by time $\tilde{T}_{\mathcal{D}}(n)$ with a constant probability. This function is a lower bound for *both* expected and high-probability latency because it only guarantees the latency of one *specific* party.
- In Section 5.2, we construct in Theorem 5.7 an adversary that ensures that

$$\hat{\sigma}^{\text{low}_\beta}[t] = \sum_{u \in \hat{A}[t]} p^{\text{low}_\beta}(t - t_u) \ge \Omega(\log\log n),$$
$$\text{for all } t \le \Theta\left(\frac{n(s^{\text{low}_\beta}(\lfloor n/\log^2 n \rfloor) - s^{\text{low}_\beta}(\lfloor \sqrt{n} \rfloor))}{\log\log n}\right).$$

  Note that Theorem 5.7 refers to *static* contention $\hat{\sigma}^{\text{low}_\beta}[t]$. Theorem 5.8 extends the lower bound of Theorem 5.7 to show that $\tilde{T}_{\mathcal{D}}(n)$ is also $\Omega\left(\frac{n(s^{\text{low}_\beta}(\lfloor n/\log^2 n \rfloor) - s^{\text{low}_\beta}(\lfloor \sqrt{n} \rfloor))}{\log\log n}\right)$. The proof is involved, and is postponed to Section 5.5. We also prove that whenever the overall latency is $O(n \log^{O(1)} n)$, there are only a small number of high-probability time slots, i.e., those i for which $p(i) > B_\beta(i)$.
- In Section 5.3, we show that

$$s^{\text{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\text{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) \ge \Omega(\log(1/q(n))).$$

  The rationale is that some party u^* inserted at time $t_{u^*} = 0$ survives to time $\tilde{T}_{\mathcal{D}}(n)$ with constant probability. In order for it to succeed by its deadline $L_{\mathcal{D}}(n, q(n))$, it must make a sufficient number of attempts in the interval $(\tilde{T}_{\mathcal{D}}(n), L_{\mathcal{D}}(n, q(n))]$. There are a sublinear number of high-probability slots that can be blocked by new wake-ups, so the remaining attempts must be counted by s^{low_β}.
- Combining the above two results, we observe the following circular relationship:
  - An improvement in the lower bound of s^{low_β} immediately leads to an improvement in the lower bound of $\tilde{T}_{\mathcal{D}}$.
  - Conversely, a stronger lower bound on $\tilde{T}_{\mathcal{D}}$ also yields a stronger lower bound on s^{low_β}.

  The process described above eventually converges to a fixed point where both bounds stabilize, and, depending on $q(n) \in \{1/2, n^{-2}\}$, implies $\Omega(n \log n / \log\log n)$ and $\Omega(n \log^2 n / \log\log n)$ lower bounds on latency In-Expectation and With-High-Probability, respectively (Theorem 5.1).
- In Section 5.4, we use a similar argument for the lower bounds: If $L^{\text{whp}}_{\mathcal{D}}(n)$ is small, then s^{low_β} must be large, which in turn implies a lower bound on the expected latency $L^{\text{exp}}_{\mathcal{D}}(n)$. This reveals the impossibility to achieve near-optimal latency, in expectation and with high probability simultaneously.

- Finally, in Section 5.5, we return to prove Theorem 5.8, by analyzing the random process induced by the adversary from Theorem 5.7. To be more specific, we use the following steps:
  - We prove that if $\sigma[t] = \Omega(\log\log n)$ for all $t \in [t_0, t_0 + \delta)$, conditioned on the observed history before t_0, then the number of successes in this interval is at most $\frac{\delta}{\log^{\Omega(1)} n}$, where $\delta = \text{polylog}(n)$. We refer to this property as the *low-density property*.
  - We divide the time slots into length δ segments, and show that if all previous segments satisfy the low-density property, then for any t in the next segment, $\sigma[t] \geq \frac{4}{5}\hat{\sigma}[t]$ when conditioned on the history of previous segments, and thus the next segment also satisfies the low-density property with high probability. This inductive step establishes that all segments are low-density with high probability. As a result, we conclude that $\sigma[t] = \Omega(\log\log n)$ holds with high probability for every t.
  - Finally, we show that the expected number of successes of a specific party u^* is at most $\log^{-\Omega(1)} n$, implying that u^* fails with probability $1 - \log^{-\Omega(1)} n$. This completes the derivation of the lower bound on $\tilde{T}_{\mathcal{D}}(n)$.

5.1 Probability Thresholds

To construct the adversary, we activate parties at random time slots so that $\mathbb{E}[\hat{\sigma}[t]] = \Omega(\log\log n)$. We then seek an implementation where $\hat{\sigma}[t] = \Omega(\log\log n)$ holds for every time slot t. However, when $p(t)$ is large, we cannot directly apply Chernoff and union bounds to obtain such an implementation, because the realized value of $\hat{\sigma}[t]$ can fall significantly below its expectation with probability $e^{-\Theta(\log\log n)} \gg n^{-1}$. On the other hand, if each random variable takes values in a small range $[0, v]$, we can strengthen the probability bound to $e^{-\Omega(\log\log n/v)} = n^{-\omega(1)}$ when v is sufficiently small. To leverage this observation, we introduce *probability thresholds*, which allow us to filter out high-probability time slots and thereby obtain tighter failure bounds.

Definition 5.1 (Filter Functions)**.** A *filter function* is a function $\mathcal{I} : \mathbb{N} \to \{0, 1\}$ that maps a *local* time index to an indicator value. Given such a function $\mathcal{I}$, a protocol $\mathcal{D}$, and an oblivious adversary $\mathcal{A}$, we define the following filtered quantities:

- $p^{\mathcal{I}}(i) = p(i)\mathcal{I}(i)$
- $s^{\mathcal{I}}(k) = \sum_{i=1}^{k} p^{\mathcal{I}}(i)$
- $\hat{\sigma}^{\mathcal{I}}[t; S] = \mathbb{E}\left[\sum_{u \in S} X^{(u)}_{t-t_u} \mathcal{I}(t - t_u)\right] = \sum_{u \in S} p^{\mathcal{I}}(t - t_u)$.
- $\sigma^{\mathcal{I}}[t; S(H_t)] = \mathbb{E}\left[\sum_{u \in S(H_t)} X^{(u)}_{t-t_u} \mathcal{I}(t - t_u)\right] = \sum_{u \in S(H_t)} p^{\mathcal{I}}(t - t_u)$.

Recall that the memoryless version of BEB is defined by $p(i) = \Theta(1/i)$. The high-probability protocol of [DS17, DKS22b] uses $p(i) = \Theta(\log i/i)$. However a general memoryless protocol does not necessarily use a p that is simple to define nor monotone decreasing. We use a filter function to filter out slots whose probability is *too large*.

Definition 5.2 (Low-probability Threshold)**.** Given a constant $\beta \geq e$, for $t \geq 1$, we define

$$B_\beta(t) = \begin{cases} 1 & t \leq 16 \\ \min(1, \frac{\ln^\beta t}{t}) & t > 16 \end{cases}.$$

For a acknowledgment-based protocol $\mathcal{D}$, we further define the following notions:

- $\mathrm{low}_\beta(t) = \mathbf{1}\{p(t) \le B_\beta(t)\}$ is the low-probability filter with respect to β and $\mathcal{D}$.
- $\mathrm{low}_\beta^{(\ge m)}(t) = \mathrm{low}_\beta(t) \cdot \mathbf{1}\{t \ge m\}$ additionally filters out time slots preceding the mth.
- Let $N^{\mathrm{high}_\beta}(k) = \sum_{t=1}^{k}(1 - \mathrm{low}_\beta(t))$ be the number of high-probability slots in the range $[1, k]$.

B_β is chosen so that $N^{\mathrm{high}_\beta}(n \log^{O(1)} n)$ can be bounded by $o(n/\log n)$, as shown in the following lemma:

Lemma 5.3. *Given $\beta \ge e$, we have the following:*

1. *$B_\beta(t) \le B_\beta(t-1)$ for $t \ge 2$. That is, $B_\beta(t)$ is monotone non-increasing.*
2. *For any protocol $\mathcal{D}$, $N^{\mathrm{high}_\beta}(k) \le s(k)/B_\beta(k) = \max(1, k \ln^{-\beta} k)s(k)$ for $k \ge 1$.*

Remark. The argument in [DS17, DKS22b] shows that $s(n) = \log^{\Theta(1)} n$ when the latency is $n \log^{O(1)} n$. Hence, $N^{\mathrm{high}_\beta}(L(n, q(n))) = o(n/\log n)$ for sufficiently large constant β.

Proof.
Proof of Part 1: We compute

$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{\ln^\beta t}{t} = \frac{(\beta - \ln t)\ln^{\beta-1} t}{t^2}.$$

This derivative is positive for $t < e^\beta$ and negative for $t > e^\beta$, so $\ln^\beta t/t$ increases on $[1, e^\beta]$ and decreases on $[e^\beta, \infty)$. Thus, $B_\beta(t)$ is non-increasing on $[e^\beta, \infty)$.

Now consider $t \in [e^e, e^\beta]$. By definition, $B_\beta(t) = 1$ if $\ln^\beta t \ge t$, which is equivalent to $\frac{\ln t}{\ln\ln t} \le \beta$. Since $\frac{\ln t}{\ln\ln t}$ increases on $[e^e, \infty)$, we have $\frac{\ln t}{\ln\ln t} \le \frac{\ln e^\beta}{\ln\ln e^\beta} = \beta/\ln\beta \le \beta$. Hence $B_\beta(t) = 1$ for all $t \in [e^e, e^\beta]$. Therefore, $B_\beta(t)$ is monotonically nonincreasing.

Proof of Part 2: For any $t \in [1, k]$, $\mathrm{low}_\beta(t) = 0$ implies $p(t) > B_\beta(t) \ge B_\beta(k)$. The number of such positions is thus at most

$$\frac{s(k)}{B_\beta(k)} = \max\left(1, \frac{k}{\ln^\beta k}\right) s(k).$$

□

To analyze the latency, we introduce the following notion:

Definition 5.3 (Restricted Time Window)**.** Given a protocol $\mathcal{D}$, we define the *restricted time window* $\tilde{T} = \tilde{T}_{\mathcal{D}}(n)$ as the largest integer $\tilde{T}$ for which there exists an adversary $\mathcal{A}$ such that:

1. there exists a party u^* activated at time 0 that succeeds in the interval $[1, \tilde{T}]$ with probability at most $1 - 4^{-1/8} \le 0.16$ under $\mathcal{A}$.
2. at most $2n/3$ parties are activated in $[0, \tilde{T}]$.

Note that $\tilde{T}_{\mathcal{D}}(n) < L_{\mathcal{D}}(n, 1/2) < L_{\mathcal{D}}(n, n^{-2})$ lower bounds both latency bounds of interest. The following simple adversary ensures no success occurs in the first $n/\log^2 n$ slots with high probability.

Lemma 5.4. *Fix any acknowledgment-based protocol $\mathcal{D}$ with $\eta = p(1) > 0$ and any sufficiently large integer $n \geq n_0(\eta)$. Then*

1. *If there exists an adversary that ensures $\hat{\sigma}[t] \geq 10 \ln n$ for $t \in [1, T_0]$ for an integer $T_0 \leq n^2$, then under this adversary, $\Pr[\exists t \in [1, T_0]. \sum_{u \in A[t]} X^{(u)}_{t-t_u} \leq 1] \leq \frac{1}{n^8}$.*
2. *There exists an adversary that uses $\lfloor n/3 \rfloor$ parties and guarantees that $\hat{\sigma}[t] \geq 10 \ln n$ for $t \in [1, \lfloor n/\ln^2 n \rfloor]$. Thus there are no successes in the interval $[1, \lfloor n/\ln^2 n \rfloor$ with high probability.*

Proof.
Proof of Part 1: By Lemma 3.1, we know:

$$\begin{aligned}\Pr\left[\exists t \in [1, T_0]. \sum_{u \in A[t]} X^{(u)}_{t-t_u} \leq 1\right] &\leq \sum_{t \in [1, T_0]} \Pr\left[\sum_{u \in A[t]} X^{(u)}_{t-t_u} \leq 1 \;\middle|\; A[t] = \hat{A}[t]\right] \\ &\leq T_0 \cdot (e^{-\sigma[t]} + \sigma[t] e^{-\sigma[t]+1}) \\ &\leq T_0 \cdot \frac{10e \ln n + 1}{n^{10}} \;\leq\; \frac{1}{n^8}.\end{aligned}$$

Proof of Part 2: We activate $\lceil 10 \ln n/\eta \rceil$ parties for each time slot $0 \leq t < \lfloor n/\ln^2 \rfloor$, then we can notice that:

- The total number of parties is $\lceil 10 \ln n/\eta \rceil \cdot \lfloor n/\ln^2 n \rfloor \leq n \cdot \frac{10 \ln n + \eta}{\eta \ln^2 n} \leq n/3$.
- For each $t \leq T_0$, $\hat{\sigma}[t] \geq \lceil 10 \ln n/\eta \rceil \cdot \eta \geq 10 \ln n$. Based on *Part 1*, we know there is no successes in $[1, \lfloor n/\ln^2 \rfloor]$ with probability at least $1 - n^{-8}$.

□

The next lemma provides the first lower bound of $\tilde{T}_{\mathcal{D}}(n)$, generalizing [DKS22b, Lemma 4.6].

Lemma 5.5. *Fix constants $\beta \geq e$, $\eta \in (0, 1]$, and error probability $q(n)$, which is either $q(n) = 1/2$ or $q(n) = n^{-2}$. For any protocol $\mathcal{D}$ with $\eta \stackrel{\text{def}}{=} p(1) > 0$, we have the following:*

1. *Trivially, $\tilde{T}_{\mathcal{D}}(n) < L_{\mathcal{D}}(n, q(n))$ for $n \geq 1$.*
2. *$\tilde{T}_{\mathcal{D}}(n) \geq \frac{s(\lfloor n/\ln^2 n \rfloor) \cdot n}{40 \ln n} \geq \frac{n}{\ln^2 n}$ for sufficiently large n.*
3. *If $L_{\mathcal{D}}(n, q(n)) = o(n \log^{\beta/2-1} n)$, then $N^{\text{high}_\beta}(\lceil n \log^{\beta/2-1} n \rceil) \leq o(n/\log n)$.*

Proof.
Proof of Part 1: By the definition of $\tilde{T}_{\mathcal{D}}(n)$, there is an adversary that with probability $4^{-1/8} \geq q(n)$, u^* does not succeed by time $\tilde{T}_{\mathcal{D}}(n)$. Therefore, $\tilde{T}_{\mathcal{D}}(n) < L_{\mathcal{D}}(n, q(n))$.

Proof of Part 2: Let $T_0 = \lfloor n/\ln^2 n \rfloor$, $T_1 = \lfloor \frac{s(T_0) \cdot n}{40 \ln n} \rfloor$. We construct an oblivious adversary $\mathcal{A}$, which partitions the parties into two sets S_1 and S_2, each of size $\lfloor n/3 \rfloor$.

The wake-up times of the parties in S_1 are assigned as in Lemma 5.4. Turning to S_2, we assign $\lfloor n/3 \rfloor$ parties wake-up times that are independent and uniformly distributed in $[0, T_1)$. Then, for each time slot $t \in (T_0, T_1]$,

$$\mathbb{E}\left[\hat{\sigma}[t]\right] \geq \sum_{u \in S_2} \mathbb{E}\left[p(t-t_u)\right] = \sum_{u \in S_2} \frac{1}{T_1} \sum_{t_u=0}^{t-1} p(t-t_u) = \frac{|S_2|}{T_1} s(t) \geq \frac{\lfloor n/3 \rfloor}{T_1} s(T_0) \geq 12 \ln n.$$

Applying a Chernoff bound (see Corollary B.3), $\Pr[\hat{\sigma}[t] \geq 4 \ln n] \geq 1 - n^{-2}$. By a union bound, $\Pr[\forall t \in (T_0, T_1].\ \hat{\sigma}[t] \geq 4 \ln n] \geq 1 - (T_1 - T_0) n^{-2} > 0$. The upshot is that there exists wake-up schedule such that $\hat{\sigma}[t] \geq 4 \ln n$ for all $t \in (T_0, T_1]$.

Now combine the assignment for S_1 and S_2. We observe that the probability of seeing *at least one* success in the interval $[1, T_1]$ remains unchanged if successful parties do not halt. That is, even previously successful $u \in \hat{A}[t]$ grab the shared resource whenever $X_{t-t_u}^{(u)} = 1$. Thus for sufficiently large n,

$$\begin{aligned}
&\Pr\left[\forall t \in [1, T_1].\ \sum_{u \in A[t]} X_{t-t_u}^{(u)} \neq 1\right] \\
&\geq 1 - \left(\sum_{t \in (T_0, T_1]} \Pr\left[\sum_{u \in \hat{A}[t]} X_{t-t_u}^{(u)} = 1\right]\right) - \left(\Pr\left[\exists t \in [1, T_0].\ \sum_{u \in A[t]} X_{t-t_u}^{(u)} \leq 1\right]\right) \\
&\geq 1 - \left(\sum_{t \in (T_0, T_1]} \sigma[t] \cdot e^{-\hat{\sigma}[t]+1}\right) - \left(\Pr\left[\exists t \in [1, T_0].\ \sum_{u \in A[t]} X_{t-t_u}^{(u)} \leq 1\right]\right)
\end{aligned}$$

By Lemma 5.4 (1) and the fact $\hat{\sigma}[t] \geq 4 \ln n$ for $t \in (T_0, T_1]$,

$$\begin{aligned}
&\geq 1 - \frac{n s(\lfloor n / \ln^2 n \rfloor)}{40 \ln n} \cdot \frac{4e \ln n}{n^4} - \frac{1}{n^8} \\
&\geq 1 - \frac{1}{n^2}.
\end{aligned}$$

Therefore, the adversary $\mathcal{A}$ wakes up at most $\frac{2}{3}n$ parties, and with probability at least $1 - \frac{1}{n^2}$, there is no success in $[1, T_1]$. This gives us a weak lower bound of $\tilde{T}_{\mathcal{D}}(n) \geq T_1 = \frac{n s(\lfloor n / \ln^2 n \rfloor)}{40 \ln n}$ for sufficiently large $n \geq n_0(\eta)$. In addition, since $s(\lfloor n / \ln^2 n \rfloor) \geq \eta$, $\frac{n \cdot s(\lfloor n / \ln^2 n \rfloor}{40 \ln n} \geq \frac{n}{\ln^2 n}$ for sufficiently large n.

Proof of Part 3: Assume n is sufficiently large. We select $n' = \Theta(n \log^{\beta/2+1} n)$ such that $\lceil n \log^{\beta/2-1} n \rceil \leq \lfloor n' / \ln^2 n' \rfloor$. By Parts 1 and 2 and the assumption that $L_{\mathcal{D}}(n, q(n)) = o(n \log^{\beta/2-1} n)$, we know

$$s(\lfloor n' / \ln^2 n' \rfloor) \leq \frac{\tilde{T}_{\mathcal{D}}(n') \cdot 40 \ln n'}{n'} \leq \frac{o(n' \log^{\beta/2-1} n') \cdot 40 \ln n'}{n'} = o(\log^{\beta/2} n'). \tag{3}$$

By Lemma 5.3, we can upper bound the number of high-probability time slots by

$$N^{\text{high}_\beta}(\lceil n \log^{\beta/2-1} n \rceil) \le N^{\text{high}_\beta}(\lfloor n'/\ln^2 n' \rfloor) \le \frac{s(\lfloor n'/\ln^2 n' \rfloor)}{B_\beta(\lfloor n'/\ln^2 n' \rfloor)}$$

According to the definition of $B_\beta(\cdot)$ and Equation (3), the above can be upper bounded by

$$\begin{aligned} &\le o(\log^{\beta/2} n') \cdot \left(\frac{\lfloor n'/\ln^2 n' \rfloor}{\ln^\beta \lfloor n'/\ln^2 n' \rfloor} \right) \\ &= o(n' \log^{-\beta/2-2} n) \;=\; o(n/\log n). \end{aligned}$$

□

5.2 Construction of the Adversary

In this subsection, we construct an adversary that maintains $\hat{\sigma}[t] = \Omega(\log\log n)$ over a longer interval, whose length depends on s^{low_β}. At this level of contention there will be *some* successes, so to bound the number of successes we need to prove that $\sigma[t]$ is also $\Omega(\log\log n)$, despite successful parties dropping out of the system and reducing the contention on future time slots.

The following general lemma shows how to construct an adversary that maintains $\hat{\sigma}[t] \ge \ell$ in a long interval and relate the length of the interval to $s^{\mathcal{I}}$.

Lemma 5.6. *We are given a protocol $\mathcal{D}$, which defines $\eta \stackrel{\text{def}}{=} p(1) > 0$, a sufficiently large $n \ge n_0(\eta)$, an integer $T_0 \in [1, n]$, a real parameter $\ell \ge 1$, and a filter function $\mathcal{I}$. Let $V = \max_{i \in [1,T_0]} p^{\mathcal{I}}(i)$. If $e^{-\ell/(7V)} < 1/n^2$, then there exists an oblivious adversary that:*

- *wakes up at most $\lfloor n/3 \rfloor$ parties.*
- *$\hat{\sigma}^{\mathcal{I}}[t] \ge \ell$ for all $t \in [T_0, T_1]$, where $T_1 \stackrel{\text{def}}{=} \left\lfloor \frac{n s^{\mathcal{I}}(T_0)}{8\ell} \right\rfloor$.*

Proof. We independently assign the activation time of the $\lfloor n/3 \rfloor$ parties to slots in $[0, T_1 - 1]$ uniformly at random, with replacement. For any time $t \in [T_0, T_1]$. The expected filtered aggregate contention at time t is

$$\mathbb{E}[\hat{\sigma}^{\mathcal{I}}[t]] = \sum_{u=1}^{\lfloor n/3 \rfloor} \frac{1}{T_1} \sum_{t_u=0}^{t-1} p^{\mathcal{I}}(t - t_u) \ge \frac{\lfloor n/3 \rfloor}{n s^{\mathcal{I}}(T_0)/(8l)} \cdot s^{\mathcal{I}}(T_0) \ge 2\ell.$$

Since the parties are activated independently, we apply a Chernoff bound (Corollary B.3) to get

$$\Pr[\hat{\sigma}^{\mathcal{I}}[t] < \ell] \le e^{-\ell/(7V)} < 1/n^2.$$

By a union bound over $[T_0, T_1]$,

$$\Pr\left[\exists t \in [T_0, T_1] \text{ such that } \hat{\sigma}^{\mathcal{I}}[t] < l\right] \le n^{-2} \left\lfloor \frac{n s^{\mathcal{I}}(T_0)}{8\ell} \right\rfloor \le n^{-2} \cdot \frac{n T_0}{8} < 1.$$

Thus, there exists an oblivious adversary such that $\hat{\sigma}^{\mathcal{I}}[t] \geq \ell$ for all $t \in [T_0, T_1]$. □

Now assume that we have a lower bound for $s^{\mathrm{low}_\beta}(n) - s^{\mathrm{low}_\beta}(\sqrt{n})$ for sufficiently large n. Consider the filter $\mathcal{I} = \mathrm{low}_\beta^{(\geq\sqrt{n})}$, where $\mathrm{low}_\beta^{(\geq\sqrt{n})}(i) = \mathrm{low}_\beta(i) \cdot \mathbf{1}\{i \geq \sqrt{n}\}$. We can construct an adversary as follows:

Theorem 5.7. *For any constants $\eta \in (0,1], \gamma > 0, \beta \geq 10$ and acknowledgment-based Contention Resolution protocol $\mathcal{D}$ satisfying $p(1) = \eta$, there exists an oblivious adversary such that for sufficiently large $n \geq n_0(\eta, \beta, \gamma)$, n_0 depending only on η, β, and γ,*

- $\hat{\sigma}[t] \geq 10 \ln n$ *for all* $t \in [1, T_0(n)]$,
- $\hat{\sigma}^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t] \geq \gamma \ln\ln n$ *for all* $t \in [T_0(n), T_1(n)]$,
- *The adversary wakes up at most $2n/3$ parties in $[1, T_1(n)]$,*

where T_0, T_1 are defined to be

$$T_0(n) \stackrel{\text{def}}{=} \lfloor n/\ln^2 n \rfloor$$
$$T_1(n) \stackrel{\text{def}}{=} \left\lfloor \frac{n s^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}(T_0(n))}{8\gamma \ln\ln n} \right\rfloor = \left\lfloor \frac{n(s^{\mathrm{low}_\beta}(\lfloor n/\ln^2 n \rfloor) - s^{\mathrm{low}_\beta}(\lfloor\sqrt{n}\rfloor))}{8\gamma \ln\ln n} \right\rfloor.$$

Proof. We assign $\lfloor n/3 \rfloor$ parties in $[0, T_0]$ as in Lemma 5.4. Let $\mathcal{I} = \mathrm{low}_\beta^{(\geq\sqrt{n})}$ and $\ell = \gamma \ln\ln n$. Since $V = \max_{t\in[1,T_0]} p^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}(t) = B_\beta(\lfloor\sqrt{n}\rfloor)$, $e^{-\ell/(7V)} = e^{-\Omega(\sqrt{n}/\,\mathrm{polylog}(n))}$, which is less than $1/n^2$ when n is sufficiently large, as a function of β, γ. Therefore, we can apply Lemma 5.6 in $[T_0, T_1]$ with $\mathcal{I} = \mathrm{low}_\beta^{(\geq\sqrt{n})}$ and $\ell = \gamma \ln\ln n$.

Combining the above two results yields the adversary satisfying the desired conditions. □

Given error probability function $q(n)$, which is either $q(n) = 1/2$ or $q(n) = n^{-2}$, we can prove that the adversary of Theorem 5.7 guarantees a low success probability for a specific party u^* in $[1, T_1(n)]$ for appropriate choice of β and γ, and therefore provides a lower bound for the *restricted time window* $\tilde{T}_{\mathcal{D}}(n)$. In particular, we have the following theorem.

Theorem 5.8. *Given a memoryless protocol $\mathcal{D}$, error probability $q(n) = 1/2$ or $q(n) = n^{-2}$, and constants $\beta \geq 10, \eta \stackrel{\text{def}}{=} p(1) > 0$, if $L_{\mathcal{D}}(n, q(n)) = o(n \log^{\beta/2-1} n)$, then for all sufficiently large n,*

$$\tilde{T}_{\mathcal{D}}(n) \geq \left\lfloor \frac{n(s^{\mathrm{low}_\beta}(\lfloor n/\ln^2 n \rfloor) - s^{\mathrm{low}_\beta}(\lfloor\sqrt{n}\rfloor))}{40\beta \ln\ln n} \right\rfloor.$$

In the interest of readability we shall postpone the proof of Theorem 5.8 to Section 5.5.

5.3 Analysis for Lower Bounds

In this section we apply Theorem 5.8 to prove Theorem 5.1. Fix a memoryless protocol $\mathcal{D}$, and recall that $L_{\mathcal{D}}^{\mathrm{whp}}(n) = L_{\mathcal{D}}(n, n^{-2})$ and $L_{\mathcal{D}}^{\exp}(n) \leq 2L_{\mathcal{D}}(n, 1/2)$. We therefore only consider $q(n) = 1/2$

when bounding expected latency and $q(n) = 1/n^2$ when bounding high-probability latency. For the sake of contradiction, we suppose that $L_{\mathcal{D}}(n, q(n)) = o(U(n))$, where $U(n) = \lfloor \frac{n \log(1/q(n)) \log n}{\log \log n} \rfloor$, which captures both claims of Theorem 5.1. When n is sufficiently large we can avoid asymptotics and proceed under the assumption that $L_{\mathcal{D}}(n, q(n)) < U(n)$. By Theorem 5.8, we know that

$$\tilde{T}_{\mathcal{D}}(n) \geq \left\lfloor \frac{n(s^{\mathrm{low}_\beta}(\lfloor n/\ln^2 n \rfloor) - s^{\mathrm{low}_\beta}(\lfloor \sqrt{n} \rfloor))}{40\beta \ln \ln n} \right\rfloor. \tag{4}$$

For memoryless protocols, we show that:

$$s^{\mathrm{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\mathrm{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) \geq \frac{1}{4} \ln(1/q(n)). \tag{5}$$

We consider the quantity $C(n) \stackrel{\text{def}}{=} \tilde{T}(n)/U(n)$. By assumption, $C(n) = o(1)$. By combining Equations (4) and (5), we obtain (informally) that $C(n) \approx 1/\ln(2/C(n))$, which leads to a contradiction.

Lemma 5.9. *Fix a memoryless protocol $\mathcal{D}$, an error probability q, which is either $q(n) = 1/2$ or $q(n) = n^{-2}$, and constants $\beta \geq 10, \eta \stackrel{\text{def}}{=} p(1) > 0$. If $L_{\mathcal{D}}(n, q(n)) = o(n \log^{\beta/2-1} n)$ then for n sufficiently large,*

$$s^{\mathrm{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\mathrm{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) \geq \frac{1}{4} \ln(1/q(n)).$$

Proof. Consider a specific party u^* activated at time 0. We will derive a lower bound of the probability that u^* does not succeed in $[1, L_{\mathcal{D}}(n, q(n))]$ and compare it with $q(n)$. We may assume that u^* does not exit after success since this does not change the probability that u^* does not succeed in $[1, L_{\mathcal{D}}(n, q(n))]$.

Let E_1 be the event that u^* does not succeed in $[1, \tilde{T}(n)]$. By the definition of $\tilde{T}_{\mathcal{D}}(n)$, there exists an adversary waking up at most $2n/3$ parties that guarantees $\Pr[E_1] \geq 4^{-1/8}$.

Next, for each high-probability time slot $t \in (\tilde{T}(n), L_{\mathcal{D}}(n, q(n))]$ for which $p(t) > B_\beta(t)$, we wake up $\lceil 4 \ln n/\eta \rceil$ parties at global time $t-1$. Let E_2 be the probability that u^* does not succeed in any of these high-probability time slots. This step wakes up at most $N^{\mathrm{high}}(L_{\mathcal{D}}(n, q(n)))\lceil 4 \ln n/\eta \rceil$ parties, guaranteeing that $\Pr[E_2] \geq 1 - 1/n \geq 4^{-1/8}$ when n is large. By Lemma 5.5(3), $N^{\mathrm{high}_\beta}(L_{\mathcal{D}}(n, q(n))) \leq N^{\mathrm{high}_\beta}(\lceil n \log^{\beta/2-1} n \rceil) = o(n/\ln n)$. Therefore, when n is sufficiently large, at most $n/3$ parties are activated in this step. Thus, at most n parties are activated in total.

Finally, let E_3 be the probability that u^* does not succeed in any of the remaining slots in $(\tilde{T}_{\mathcal{D}}(n), L_{\mathcal{D}}(n, q(n))]$. Since $p^{\mathrm{low}_\beta}(t) \leq B_\beta(t) = \frac{\ln^\beta t}{t}$ and $\tilde{T}_{\mathcal{D}}(n) \geq \Omega(n/\ln^2 n)$ by Lemma 5.5, we may assume $p^{\mathrm{low}_\beta}(t) \leq 1/2$ for all $\tilde{T}_{\mathcal{D}}(n) < t \leq L_{\mathcal{D}}(n, q(n))$ when n is sufficiently large. Using the approximation $1 - x \geq 4^{-x}$ for $x \in [0, 1/2]$, we have

$$\Pr[E_3] = \prod_{t \in (\tilde{T}_{\mathcal{D}}(n), L_{\mathcal{D}}(n, q(n))]} (1 - p^{\mathrm{low}_\beta}(t)) \geq (1/4)^{s^{\mathrm{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\mathrm{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)))}.$$

Since the protocol is memoryless, E_1, E_2, E_3 are independent. Thus, the probability that u^* does not succeed in $[1, L_{\mathcal{D}}(n, q(n))]$ is $\Pr[E_1] \Pr[E_2] \Pr[E_3] \geq 4^{-(s^{\mathrm{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\mathrm{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) + 1/4)}$.

Since u^* succeeds before $L_{\mathcal{D}}(n, q(n))$ with probability at least $1 - q(n)$, we must have

$$4^{-(s^{\text{low}_\beta}(L_{\mathcal{D}}(n,q(n)))-s^{\text{low}_\beta}(\tilde{T}_{\mathcal{D}}(n))+1/4)} \leq q(n).$$

It follows that

$$s^{\text{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\text{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) \geq \frac{\ln(1/q(n))}{\ln 4} - 1/4 \geq \frac{1}{4}\ln(1/q(n)).$$

□

The following lemma summarizes the statements we need for the final lower bound.

Lemma 5.10. *Given a error probability function $q(n)$ that is either identically $= 1/2$ or identically n^{-2}, let $\beta = 10$ and $U(n) = \left\lfloor \frac{n \ln(1/q(n)) \ln n}{\ln \ln n} \right\rfloor$. If $L_{\mathcal{D}}(n, q(n)) = o(U(n))$, then there exists an integer n_0 such that the following statements hold when $n \geq n_0$:*

(i) $\tilde{T}_{\mathcal{D}}(n) \geq \left\lfloor \frac{n(s^{\text{low}_\beta}(\lfloor n/\ln^2 n \rfloor) - s^{\text{low}_\beta}(\lfloor \sqrt{n} \rfloor))}{40\beta \ln \ln n} \right\rfloor$.

(ii) $\tilde{T}_{\mathcal{D}}(n) \geq n/\ln^2 n$.

(iii) $L_{\mathcal{D}}(n, q(n)) > \tilde{T}_{\mathcal{D}}(n)$.

(iv) $U(n) > L_{\mathcal{D}}(n, q(n))$.

(v) $\max\{U(n') : U(n') \leq cU(n)\} \geq cU(n)/2$ *whenever* $20/n \leq c < 1$.

(vi) $s^{\text{low}_\beta}(L_{\mathcal{D}}(n, q(n))) - s^{\text{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) \geq \frac{1}{4}\ln(1/q(n))$.

(vii) $U(n) \leq \lfloor n \ln^2 n \rfloor$.

(viii) $\ln(1/q(\sqrt{n})) \geq \frac{1}{3}\ln(1/q(n))$.

(ix) $\frac{\ln \ln i}{\ln(1/q(i)) \ln^3 i} \geq \frac{\ln \ln n}{\ln(1/q(n)) \ln^3 n} \geq 1/\ln^4(\sqrt{n}) \geq 20/\sqrt{n}$ *for all* $i \leq n$.

(x) $U(i) \leq U(n)$ *for all* $1 \leq i \leq n$.

(xi) $\ln(\lfloor n/\ln^4 n \rfloor/(\sqrt{n} \ln^4 \sqrt{n})) \geq \frac{1}{5}\ln n$.

Proof. Items (i)–(iii) and (vi) follow from Theorem 5.8, Lemma 5.5 (ii), Definition 5.3, and Lemma 5.9, respectively. See Appendix C.2 for technical lemmas that imply Item (v). Item (iv) is a consequence of the assumption that $L_{\mathcal{D}}(n, q(n)) = o(U(n))$. Items (vii)–(xii) are straightforward mathematical facts. □

We are now ready to prove Theorem 5.1. To prove both the In-Expectation and With-High-Probability lower bounds of Theorem 5.1, it suffices to show that no protocol $\mathcal{D}$ has latency $L_{\mathcal{D}}(n, q(n)) = o(\frac{n \log(1/q(n)) \log n}{\log \log n})$, where the error function is either $q(n) = 1/2$ or $q(n) = 1/n^2$.

Proof of Theorem 5.1. Take $\beta = 10$, and recall that $U(n) = \left\lfloor \frac{n \ln(1/q(n)) \ln n}{\ln \ln n} \right\rfloor$. Suppose, for the sake of obtaining a contradiction, that $L_{\mathcal{D}}(n, q(n)) = o(U(n))$. We choose n_0 as in Lemma 5.10 and henceforth assume $n \geq n_0^2$.

Let $C(n) = \tilde{T}_{\mathcal{D}}(n)/U(n)$, which is $o(1)$ since $\tilde{T}_{\mathcal{D}}(n) < L_{\mathcal{D}}(n, q(n)) = o(U(n))$. It follows that $\ln(2/C(n)) = o(C(n)^{-1})$. By Lemma 5.10(ii), $\tilde{T}_{\mathcal{D}}(n) \geq n/\ln^2 n$ and we also have $C(n) \geq \frac{\ln \ln n}{\ln(1/q(n)) \ln^3 n}$. We define numbers N_0, C_0, N as follows.

- Let $N_0 \geq n_0$ be a constant such that $2400\beta \ln(2/C(n)) \leq (2C(n))^{-1}$ for all $n \geq N_0$. The existence of N_0 is due to our assumption $C(n) = o(1)$ and the fact that $\ln(1/x) = o(1/x)$ for small x.
- Let $C_0 = \min_{N_0 \leq n \leq N_0^2} C(n)$. By the definition of N_0 we have $2400\beta \ln(2/C_0) \leq (2C_0)^{-1}$.
- Let $N = \min\{N' : N' \geq N_0, C(N') < C_0\}$ be the smallest integer that is not smaller than N_0 and satisfies $C(N) < C_0$. The existence of N is due to our assumption $C(n) = o(1)$.

We prove that $C(N) \geq C_0$, which contradicts the definition of N. By the definition of C_0 and N, $N > N_0^2$ and $C(n) \geq C_0$ for all $\sqrt{N} \leq n < N$. Define the sequence (N_i) by $N_1 = \lfloor N/\ln^4 N \rfloor$ and for $i > 1$, $N_i = \arg\max_{N'}\{U(N') \leq C_0 U(N_{i-1})\}$. We terminate the sequence at $i_{\max}$, defined to be

$$i_{\max} = \min\{i : \min(C_0 U(N_i), N_i) \leq \sqrt{N}\}.$$

By the definition of C_0, we have:

$$1 > C_0 = \min_{N_0 \leq n \leq N_0^2} C(n) = \min_{N_0 \leq n \leq N_0^2} \left(\frac{\tilde{T}(n)}{U(n)} \right)$$

By Lemma 5.10(ii) this is lower bounded by

$$\geq \min_{N_0 \leq n \leq N_0^2} \left(\frac{n/\ln^2 n}{n \ln(1/q(n)) \cdot \ln n / \ln \ln n} \right)$$

Applying Lemma 5.10(ix),

$$\geq \frac{\ln \ln(N_0^2)}{\ln(1/q(N_0^2)) \cdot \ln^3(N_0^2)} \geq \frac{1}{\ln^4 N_0}$$

Since $N \geq N_0^2$, we have:

$$C_0 \geq \frac{1}{\ln^4(\sqrt{N})} \tag{6}$$

Since $\frac{1}{\ln^4 \sqrt{N}} \geq \frac{20}{\sqrt{N}} \geq \frac{20}{N_{i-1}}$ by Lemma 5.10 (ix), applying Lemma 5.10(v), we have $U(N_i) \geq C_0 U(N_{i-1})/2$ for $2 \leq i \leq i_{\max}$, and by the definition of $i_{\max}$ we have

$$\min(C_0 U(N_{i_{\max}}), N_{i_{\max}}) \leq \sqrt{N}.$$

If this last inequality is satisfied because $C_0U(N_{i_{\max}}) \le \sqrt{N}$, then by Equation (6), we have:

$$U(N_{i_{\max}}) \le \sqrt{N}/C_0 \le \sqrt{N}\ln^4\sqrt{N}.$$

If it were satisfied because $N_{i_{\max}} \le \sqrt{N}$, then by Lemma 5.10(x) and the definition of $U(\cdot)$,

$$U(N_{i_{\max}}) \le U(\sqrt{N}) \le \sqrt{N}\ln^4\sqrt{N}.$$

Therefore, in every case $U(N_{i_{\max}}) \le \sqrt{N}\ln^4\sqrt{N}$. By Lemma 5.10(xi),

$$\begin{aligned} i_{\max} - 1 &\ge \frac{\ln(U(N_1)/U(N_{i_{\max}}))}{\ln(\max_{1\le i\le i_{\max}-1} U(N_{i+1})/U(N_i))} \\ &\ge \frac{\ln(\lfloor N/\ln^4 N\rfloor/(\sqrt{N}\ln^4\sqrt{N}))}{\ln(2/C_0)} \\ &\ge \frac{\ln N}{5\ln(2/C_0)}. \end{aligned}$$

For $i \in [1, i_{\max}]$, since $n_0 \le N_0 \le \sqrt{N}$, we have $\tilde{T}_{\mathcal{D}}(N_i) = C(N_i)\cdot U(N_i) \ge C_0U(N_i)$. By Lemma 5.10(vi,viii), we have:

$$\begin{aligned} s^{\mathrm{low}_\beta}(U(N_i)) - s^{\mathrm{low}_\beta}(C_0U(N_i)) &\ge s^{\mathrm{low}_\beta}(L_{\mathcal{D}}(N_i, q(N_i))) - s^{\mathrm{low}_\beta}(\tilde{T}_{\mathcal{D}}(N_i)) \\ &\ge \frac{1}{4}\ln(1/q(N_i)) \ge \frac{1}{4}\ln(1/q(\lfloor\sqrt{N}\rfloor)) \ge \frac{1}{12}\ln(1/q(N)). \end{aligned}$$

Since the intervals $(C_0U(N_i), U(N_i)]$ are disjoint and are in $(\lfloor\sqrt{N}\rfloor, \lfloor N/\ln^2 N\rfloor]$, we have

$$\begin{aligned} s^{\mathrm{low}_\beta}(\lfloor N/\ln^2 N\rfloor) - s^{\mathrm{low}_\beta}(\lfloor\sqrt{N}\rfloor) &\ge \sum_{i=1}^{i_{\max}-1}\left[s^{\mathrm{low}_\beta}(U(N_i)) - s^{\mathrm{low}_\beta}(C_0U(N_i))\right] \\ &\ge (i_{\max}-1)\cdot\frac{1}{12}\ln(1/q(N)) \ge \frac{\ln N}{5\ln(2/C_0)}\cdot\frac{1}{12}\ln(1/q(N)) \\ &\ge \frac{U(N)\ln\ln N}{60\ln(2/C_0)N}. \end{aligned}$$

It follows that

$$\begin{aligned} \tilde{T}_{\mathcal{D}}(N) &\ge \left\lfloor \frac{n(s^{\mathrm{low}_\beta}(\lfloor N/\ln^2 N\rfloor) - s^{\mathrm{low}_\beta}(\lfloor\sqrt{N}\rfloor))}{40\beta\ln\ln N} \right\rfloor \\ &\ge \lfloor \frac{U(N)}{2400\beta\ln(2/C_0)} \rfloor \ge \lfloor 2C_0U(N)\rfloor \\ &\ge C_0U(N). \end{aligned}$$

The third inequality follows from the condition $2400\beta\ln(2/C_0) \le (2C_0)^{-1}$, as specified in the definition of C_0. Therefore, $C(N) = \tilde{T}_{\mathcal{D}}(N)/U(N) \ge C_0$, contradicting our choice of N. □

5.4 Tradeoff Between Expected Latency and High-probability Latency

By applying an argument that is similar to Theorem 5.1, we can prove the tradeoff lower bound of Theorem 1.5, which states that no memoryless protocol $\mathcal{D}$ has both $L_{\mathcal{D}}^{\exp}(n) = o(\frac{n \log^2 n}{(\log \log n)^2})$ and $L_{\mathcal{D}}^{\text{whp}}(n) = n \log^{O(1)} n$.

Proof of Theorem 1.5. Suppose $L_{\mathcal{D}}^{\text{whp}}(n) \le \bar{U}(n) = n \ln^{\beta/2-1} n$ for some constant $\beta \ge 10$.

By Lemma 5.5(2), we know $\tilde{T}_{\mathcal{D}}(n) \ge n/\ln^2 n$ for sufficiently large n. By Lemma 5.9,

$$\begin{aligned} s^{\text{low}_\beta}(\lfloor n \ln^{\beta/2-1} n \rfloor) - s^{\text{low}_\beta}(\lfloor n/\ln^2 n \rfloor) &\ge s^{\text{low}_\beta}(L_{\mathcal{D}}(n, n^{-2})) - s^{\text{low}_\beta}(\tilde{T}_{\mathcal{D}}(n)) \\ &\ge \frac{1}{4} \ln(1/(n^{-2})) \ge \frac{1}{2} \ln n. \end{aligned}$$

We define $\bar{C}_0 = \min_{\sqrt{n} \le t \le n} \left(\frac{\tilde{T}_{\mathcal{D}}(n)}{\bar{U}(n)} \right)$, then we have

$$\bar{C}_0 \ge \min_{\sqrt{n} \le t \le n} \frac{\lfloor t/\ln^2 t \rfloor}{\lfloor t \ln^{\beta/2-1} t \rfloor} \ge \ln^{-\beta/2-2} n \quad \text{for sufficiently large } n \tag{7}$$

. We choose a series of thresholds $\{n_i\}_{1 \le i \le i_{\max}}$ such that $n_1 = \lfloor n/\ln^4 n \rfloor$, $n_i = \arg\max_{n'} \{\bar{U}(n') \le \bar{C}_0 \bar{U}(n_{i-1})\}$ for $i \ge 2$, and

$$i_{\max} = \min\{i : \min(C(n)U(n_i), n_i) \le \sqrt{n}\}.$$

We can notice that:

- If $C_0 U(n_{i_{\max}}) \le \sqrt{n}$, then by Equation (7), $U(n_{i_{\max}}) \le \sqrt{n}/\bar{C}_0 \le \sqrt{n} \cdot \ln^{\beta/2+2} n$.
- Otherwise, $n_{i_{\max}} \le \sqrt{n}$, then $\bar{U}(n_{i_{\max}}) \le \bar{U}(\lfloor \sqrt{n} \rfloor) \le \sqrt{n} \ln^{\beta/2+2} n$.

Thus we have:

$$U(n_{i_{\max}}) \le \sqrt{n} \ln^{\beta/2+2} n \quad \text{for sufficiently large } n \tag{8}$$

For sufficiently large n and $2 \le i \le i_{\max}$, by the fact $\bar{U}(n_i+1)/\bar{U}(n_{i-1}) > \bar{C}_0$ and Equation (7), we can notice that:

$$\begin{aligned} \bar{U}(n_i)/\bar{U}(n_{i-1}) &= \left(\frac{\bar{U}(n_i+1)}{\bar{U}(n_i+1)} \right) - \left(\frac{\bar{U}(n_i+1) - \bar{U}(n_i)}{\bar{U}(n_{i-1})} \right) \\ &\ge \bar{C}_0 - O(\ln^{\beta/2-1} n)/\Omega(\sqrt{n} \cdot \ln^{\beta/2+2} n) \\ &\ge \bar{C}_0 - O(1/\sqrt{n}) \\ &\ge \bar{C}_0/2 \end{aligned} \tag{9}$$

and by Equation (8) and Equation (9),

$$\begin{aligned} i_{\max} - 1 &\geq \frac{\ln(\bar{U}(n_1)/\bar{U}(n_{i_{\max}}))}{\ln(\max_{2\leq i\leq i_{\max}} \bar{U}(n_{i-1})/\bar{U}(n_i))} \\ &\geq \frac{\ln(\lfloor n/\ln^4 n\rfloor/(\sqrt{n}\ln^{\beta/2+2} n))}{\ln(2/\bar{C}_0)} \\ &\geq \Omega\left(\frac{\log n}{\log\log n}\right). \end{aligned}$$

Lastly, by the definition of $\bar{C}_0$, we know $\bar{C}_0\bar{U}(n_i) \leq \bar{T}_{\mathcal{D}}(n)$ so $(\bar{C}_0\bar{U}(n_i), \bar{U}(n_i)]\,(1 \leq i < i_{\max})$ are disjoint intervals. Therefore,

$$\begin{aligned} s^{\text{low}_\beta}(\lfloor n/\ln^2 n\rfloor) - s^{\text{low}_\beta}(\lfloor\sqrt{n}\rfloor) &\geq \sum_{i=1}^{i_{\max}-1} \left[s^{\text{low}_\beta}(U(n_i)) - s^{\text{low}_\beta}(\bar{C}_0 \cdot \bar{U}(N_i))\right] \\ &\geq (i_{\max} - 1) \cdot \frac{1}{2}\ln n_i \geq \Omega\left(\frac{\log^2 n}{\log\log n}\right). \end{aligned}$$

Applying Theorem 5.8,

$$L^{\text{exp}}_{\mathcal{D}}(n) \geq \tilde{T}_{\mathcal{D}}(n) \geq \left\lfloor \frac{n(s^{\text{low}_\beta}(\lfloor n/\ln^2 n\rfloor) - s^{\text{low}_\beta}(\lfloor\sqrt{n}\rfloor))}{40\beta \ln\ln n} \right\rfloor = \Omega\left(\frac{n\log^2 n}{(\log\log n)^2}\right).$$

□

5.5 Proof of Theorem 5.8

Recall that Theorem 5.7 gave an adversary that sustains a high *static* contention $\hat{\sigma}^{\mathcal{I}}[t] = \Omega(\log\log n)$ over a certain interval of time, for the filter $\mathcal{I} = \text{low}_\beta^{(\geq\sqrt{n})}$. This does not *directly* imply a similar lower bound $\sigma^{\mathcal{I}}[t] = \Omega(\log\log n)$, as parties achieving success *reduce* the dynamic contention on future time slots.

The idea of the proof of Theorem 5.8 is as follows. We divide the time slots into intervals of length $\delta = \log^{\Theta(1)} n$. If $\sigma^{\mathcal{I}}[t] = \Omega(\log\log n)$ in an interval, then there will be few successes in that interval with very high probability. If there are few successes in previous intervals, then the difference between $\sigma^{\mathcal{I}}[t]$ and $\hat{\sigma}^{\mathcal{I}}[t]$ caused by these successes is negligible. By using the filter $\mathcal{I} = \text{low}_\beta^{(\geq\sqrt{n})}$ that removes all high probability slots, we guarantee that $\sigma^{\mathcal{I}}[t]$ does not decrease much within an interval. Consequently, we have $\sigma^{\mathcal{I}}[t] \approx \hat{\sigma}^{\mathcal{I}}[t] = \Omega(\log\log n)$ in the next interval. By induction, we can prove $\sigma^{\mathcal{I}}[t] = \Omega(\log\log n)$ for all $t \in [1, T]$ with high probability, provided that $\hat{\sigma}^{\mathcal{I}}[t] = \Omega(\log\log n)$ initially, for all $t \in [1, T]$. Then, the expected number of successes of a specific party u^* activated at time 0 is at most $s(T)/e^{\Omega(\log\log n)} = \log^{-\Omega(1)} n$ for appropriately chosen constants. It follows that the success probability of u^* is at most $\log^{-\Omega(1)} n$, which yields a lower bound $T \leq \tilde{T}_{\mathcal{D}}(n)$.

We begin with some definitions specific to this section.

Definition 5.4 (Success Record, (μ, I)-Goodness, Density Profiles)**.**

1. Define $\text{Succ}[t] \stackrel{\text{def}}{=} \hat{A}[t] \setminus A[t]$ as the set of parties that have succeeded by global time t. Recall

that $A[t \mid t']$ is the set of parties that are activated by time t and yet to succeed by time t'. By this definition, we have $A[t \mid t'] = \hat{A}[t] \setminus \mathrm{Succ}[t']$, for $t' \le t$.

2. Define the *success record* by global time t as $\mathrm{Rec}[t] = \{(u, t_u^{\mathrm{succ}}) : u \in \mathrm{Succ}[t]\}$, i.e., the set of successful parties along with their success time by global time t. By abuse of notation, we write $u \in \mathrm{Rec}[t]$ to mean that there exists a pair $(u, \tau) \in \mathrm{Rec}[t]$ for some τ.

3. A success record R is said to be (μ, I)-*good* for a real number $\mu \in [0, 1]$ and a set of time slots I if the number of successes in I is at most $\mu|I|$. That is, the success *density* in I is low.

4. A *density profile* Π is a collection of pairs (μ, I), where $\mu \in [0, 1]$ is a real number and I is an interval of time slots. A success record R is said to be Π-*good* if it is (μ, I) good for every $(\mu, I) \in \Pi$.

5. For integers $t_0, \delta \ge 1$ and real number $\mu \in [0, 1]$, the (t_0, μ, δ)-*density profile* $\Pi(t_0, \mu, \delta)$ is defined as follows:

   - $I_0 = [1, t_0)$ with density $\mu_0 = 0$;
   - For $i \ge 1$, let $I_i = [t_0 + (i-1)\delta, t_0 + i\delta)$ and $\mu_i = \mu$;
   - Then $\Pi(t_0, \mu, \delta) = \{(\mu_i, I_i)\}$.

   That is, we divide the time slots into intervals of length δ except the first interval $[1, t_0)$, and require no success in the first interval and at most $\mu\delta$ successes in other intervals.

6. A success record R is said to be (t_0, μ, δ)-*good* if it is $\Pi(t_0, \mu, \delta)$-good.

We restate our plan as follows:

- In Section 5.5.1, we show that if $\sigma^{\mathcal{I}}[t; A[t \mid t_0]] = \Omega(\log\log n)$ for all $t \in [t_0, t_0 + \delta)$, then the success record is $(2\mu, I)$-good with high probability where $\mu \approx \log^{-\Omega(1)} n$ and $I = [t_0, t_0 + \delta)$.
- Section 5.5.2 shows that if the success record is (μ_i, I_i)-good for all $i < k$ where $(\mu_i, I_i) \in \Pi(t_0, 2\mu, \delta)$, then it is also (μ_k, I_k)-good with high probability, provided that $\hat{\sigma}^{\mathcal{I}}[t] = \Omega(\log\log n)$ in I_k. By induction, an adversary satisfying the properties in Theorem 5.7 guarantees that the success record $\mathrm{Rec}[T]$ is $(t_0, 2\mu, \delta)$-good with high probability, and hence $\sigma^{\mathcal{I}}[t] = \Omega(\log\log n)$ for all $t \in [1, T]$ with high probability.
- Finally, we show that the expected number of successes of a particular party u^* is $\log^{-\Omega(1)} n$, thus concluding the lower bound of $\tilde{T}(n)$. Details are provided in Section 5.5.3.

The following fact is useful:

Fact 5.11. *For any memoryless protocol $\mathcal{D}$, filter $\mathcal{I}$, and time $t_0 \le t$,*

$$\sigma^{\mathcal{I}}[t; A[t \mid t_0]] = \hat{\sigma}^{\mathcal{I}}[t] - \sigma^{\mathcal{I}}[t; \mathrm{Succ}[t_0]].$$

Lemma 5.12 (Generalization of Lemma 3.1(2).)**.** *For any filter $\mathcal{I}$ and time slot t,*

$$\Pr\left[\sum_{u \in A[t]} X^{(u)}_{t - t_u} = 1\right] \le (1 + e \cdot \sigma^{\mathcal{I}}[t]) e^{-\sigma^{\mathcal{I}}[t]}.$$

Proof. The proof is similar to Lemma 3.1(2). Since $X^{(u)}_{t-t_u} \geq X^{(u)}_{t-t_u}\mathcal{I}(t-t_u)$,

$$\Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u} = 1\right] \leq \Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) \leq 1\right] \tag{10}$$

Since $X^{(u)}_{t-t_u}$ ($u \in A[t]$) are mutually independent,

$$\Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) = 0\right] = \prod_{u\in A[t]}\left(1 - \Pr\left[X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) = 1\right]\right) \leq e^{-\sigma^{\mathcal{I}}[t]} \tag{11}$$

and

$$\begin{aligned}
&\Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) = 1\right] \\
&= \sum_{v\in A[t]} \Pr\left[X^{(v)}_{t-t_v}\mathcal{I}(t-t_v) = 1\right] \prod_{u\in A[t]\setminus\{v\}}\left(1 - \Pr\left[X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) = 1\right]\right) \\
&\leq \sum_{v\in A[t]} \Pr[X^{(v)}_{t-t_v}\mathcal{I}(t-t_v) = 1]e^{-\sigma^{\mathcal{I}}[t]+1} = \sigma^{\mathcal{I}}[t]e^{-\sigma^{\mathcal{I}}[t]+1}.
\end{aligned} \tag{12}$$

Combining Equations (10) to (12), we have:

$$\begin{aligned}
\Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) \leq 1\right] &= \Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) = 0\right] + \Pr\left[\sum_{u\in A[t]} X^{(u)}_{t-t_u}\mathcal{I}(t-t_u) = 1\right] \\
&\leq (1 + e\cdot\sigma^{\mathcal{I}}[t])e^{-\sigma^{\mathcal{I}}[t]}.
\end{aligned}$$

□

5.5.1 Proving $(2\mu, I)$-goodness

If $\sigma[t; A[t \mid t_0]]$ is large for all $t \in [t_0, t_0+\delta)$, then there are few successes in this interval. To prove this, we first introduce the following lemma, which shows that the loss in $\sigma^{\mathrm{low}^{(\geq\sqrt{n})}_{\beta}}[t]$ caused by successes in a short interval is small.

Lemma 5.13. *For any memoryless protocol $\mathcal{D}$, integers t_0, δ, t with $t \geq t_0 + \delta$,*

$$\sigma^{\mathrm{low}^{(\geq\sqrt{n})}_{\beta}}[t; A[t \mid t_0+\delta]] \geq \sigma^{\mathrm{low}^{(\geq\sqrt{n})}_{\beta}}[t; A[t \mid t_0]] - B_\beta(\sqrt{n})\delta.$$

Proof. Each party can contribute at most $B_\beta(\sqrt{n})$ to $\sigma^{\mathrm{low}^{(\geq\sqrt{n})}_{\beta}}[t; A[t \mid t_0+\delta]]$, and there are at most δ parties that succeed in $[t_0, t_0+\delta)$. The statement follows. □

Lemma 5.14. *Fix a memoryless protocol $\mathcal{D}$ and integers $t_0, \delta \geq 1, \ell \geq 2$. Suppose $\sigma^{\mathrm{low}^{(\geq\sqrt{n})}_{\beta}}[t; A[t \mid t_0]] \geq \ell$ for all $t \in [t_0, t_0+\delta)$ and $B_\beta(\sqrt{n})\delta \leq \ell/2$. Then, conditioned on H_{t_0}, the success record is $(2\mu, I)$-good with probability at least $1 - e^{-\mu\delta/3}$, where $\mu = (1 + (e\cdot\ell/2))e^{-(\ell/2)})$ and $I = [t_0, t_0+\delta)$.*

Proof. By Lemma 5.13 and our assumptions that $\sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; A[t \mid t_0]] \geq \ell$ and $B_\beta(\sqrt{n})\delta \leq \ell/2$,

$$\begin{aligned}\sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; A[t]] &\geq \sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; A[t \mid t_0]] - (t - t_0)B_\beta(\sqrt{n}) \\ &\geq \sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; A[t \mid t_0]] - \delta \cdot B_\beta(\sqrt{n}) \\ &\geq \ell/2.\end{aligned}$$

Then, by Lemma 5.12, the success probability at time t is at most $\mu = (1 + e \cdot \ell/2)e^{-\ell/2}$. Hence, the expected number of successes in $[t_0, t_0 + \delta)$ is at most $\mu\delta$. Moreover, since the probability bound is independent of the history within the interval $[t_0, t)$, we can apply the Chernoff bound (Corollary B.3). It follows that the probability of more than 2μ successes is at most $e^{-\mu\delta/3}$. □

5.5.2 Proving $(t_0, 2\mu, \delta)$-goodness and High-contention

We now jointly establish, with high probability, that under the adversary constructed in Theorem 5.7, the success record is $(t_0, 2\mu, \delta)$-good for appropriate parameters t_0, μ, δ, and that $\sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t] = \Omega(\log\log n)$ also holds. Let I_i be the ith interval in the density profile $\Pi(t_0, \mu, \delta)$ (Recall that $I_0 = [1, t_0)$ and $I_i = [t_0 + (i-1)\delta, t_0 + i\delta)$). We first show that if the success record is good, then the contention loss due to successes is small.

Lemma 5.15. *Given parameters $t' \leq t, \delta \geq e^\beta, \mu > 0$, if $\mathrm{Rec}[t']$ is (t_0, μ, δ)-good, then*

$$\sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; \mathrm{Succ}[t']] \leq 3B_\beta(\sqrt{n})\delta + \frac{\mu \ln^{\beta+1} t}{\beta + 1}.$$

Proof. By definition,

$$\sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; \mathrm{Succ}[t']] = \sum_{u \in \mathrm{Succ}[t']} p^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}(t - t_u).$$

Suppose $t \in I_k$. If a party $u \in \mathrm{Succ}[t']$ succeeds at time t_u^{succ}, then $t_u < t_u^{\mathrm{succ}}$ and $p^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}(t - t_u) \leq B_\beta(\max(t - t_u^{\mathrm{succ}}, \sqrt{n}))$. So the contribution of parties that succeeded in I_i for each $i \leq k-3$ is at most $\mu\delta \cdot B_\beta((k-i-1)\delta)$. For $i \in \{k-2, k-1, k\}$, their total contribution is at most $3\delta \cdot B_\beta(\sqrt{n})$. So

$$\begin{aligned}\sigma^{\mathrm{low}_\beta^{(\geq\sqrt{n})}}[t; \mathrm{Succ}[t']] &\leq 3\delta \cdot B_\beta(\sqrt{n}) + \mu\delta \sum_{i=2}^{k-1} \frac{\ln^\beta(i\delta)}{i\delta} \\ &\leq 3\delta \cdot B_\beta(\sqrt{n}) + \mu \int_\delta^t \frac{\ln^\beta x}{x} \mathrm{d}x \\ &\leq 3\delta \cdot B_\beta(\sqrt{n}) + \frac{\mu \ln^{\beta+1} t}{\beta + 1}.\end{aligned}$$

□

Lemma 5.16. *Let n be sufficiently large, $t_0 = \lfloor n/\ln^2 n \rfloor$, $\delta = \lfloor \ln^{2\beta+4} n \rfloor$ and $\mu = (1 + e \cdot 2\beta \ln\ln n)e^{-2\beta \ln\ln n}$. Suppose there exists an adversary $\mathcal{A}[n]$ and an integer T with $t_0 < T \le n^2$ such that*

- $\hat{\sigma}[t] \ge 10 \ln n$ *for all* $t \in [1, t_0]$, *and*
- $\hat{\sigma}^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t] \ge 5\beta \ln\ln n$ *for all* $t \in (t_0, T]$.

Then for any $k \ge 1$, the following hold:

1. *Let E_i be the event that the success record is $(2\mu, I_i)$-good. If events $E_0, E_1, \ldots, E_{k-1}$ all happen, then for any $t \in I_k \cap [1, T]$, $\sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; A[t \mid t_0 + (k-1)\delta]] \ge \sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t] \ge 4\beta \ln\ln n$.*
2. *If $I_k \subseteq [t_0, T]$, then $\Pr[E_k \mid E_0 \cap E_1 \cap \cdots \cap E_{k-1}] \ge 1 - e^{-\ln^3 n}$. As a consequence, $\Pr[E_0 \cap E_1 \cdots \cap E_k] \ge 1 - n^{-6} - k \cdot e^{-\ln^3 n} \ge 1 - 2n^{-6}$, and $\Pr\left[\sigma^{\mathrm{low}_\beta^{(\sqrt{n})}}[t] \ge 4\beta \ln\ln n\right] \ge 1 - 2n^{-6}$ for all $t \in [t_0, T]$.*

Proof. Suppose E_i happens for all $i < k$. Then $\mathrm{Rec}[t_0 + (k-1)\delta]$ is $(t_0, 2\mu, \delta)$-good. By Lemma 5.15, Fact 5.11 and Lemma 5.13, for any $t \in I_k \cap [1, T]$,

$$\begin{aligned}
\sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; A[t]] &\ge \sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; A[t \mid t_0 + (k-1)\delta]] - B_\beta(\sqrt{n})\delta \\
&\ge \hat{\sigma}^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t] - \sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; \mathrm{Succ}[t_0 + (k-1)\delta]] - B_\beta(\sqrt{n})\delta \\
&\ge \hat{\sigma}^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t] - \left(3B_\beta(\sqrt{n})\delta + \frac{\mu \ln^{\beta+1} t}{\beta+1}\right) - B_\beta(\sqrt{n})\delta \\
&\ge 5\beta \ln\ln n - 4B_\beta(\sqrt{n})\delta - \frac{\mu \ln^{\beta+1} t}{\beta+1}.
\end{aligned}$$

For sufficiently large n, we have $B_\beta(\sqrt{n}) = \frac{\ln^\beta \sqrt{n}}{\sqrt{n}}$ and $\mu \le \ln^{-2\beta+1} n \le \ln^{-2\beta+1} n^2$. We also have $t \le T \le n^2$ by our assumption. Thus,

$$4B_\beta(\sqrt{n})\delta + \frac{\mu \ln^{\beta+1} t}{\beta+1} \le \frac{4\ln^\beta \sqrt{n}}{\sqrt{n}} \ln^{2\beta+4} n + \frac{\ln^{2-\beta} n^2}{\beta+1} = o(1).$$

So $\sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; A[t \mid t_0 + (k-1)\delta]] \ge \sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; A[t]] \ge 4\beta \ln\ln n$.

By Lemma 5.14, if $\sigma^{\mathrm{low}_\beta^{(\ge\sqrt{n})}}[t; A[t \mid t_0 + (k-1)\delta]] \ge 4\beta \ln\ln n$ for all $t \in I_k$, then E_k happens with probability at least $1 - e^{-\mu\delta/3} \ge 1 - e^{-\ln^3 n}$ when n is sufficiently large. So $\Pr[E_i \mid E_0 \cap E_1 \cap \cdots \cap E_{i-1}] \ge 1 - e^{-\ln^3 n}$.

Next, we prove by induction that $\Pr[E_0 \cap E_1 \cap \cdots \cap E_k] \ge 1 - n^{-6} - k \cdot e^{-\ln^3 n} \ge 1 - 2n^{-6}$ when n is large enough. The base case $\Pr[E_0] \ge 1 - n^{-6}$ because of the fact that $\hat{\sigma}[t] \ge 10 \ln n$ for $t \le t_0$ and Lemma 5.4. Then for $k \ge 1$,

$$\begin{aligned}
\Pr[E_0 \cap E_1 \cap \cdots \cap E_k] &= \Pr[E_0 \cap E_1 \cap \cdots \cap E_{k-1}] \Pr[E_k \mid E_0 \cap E_1 \cap \cdots \cap E_{k-1}] \\
&\ge (1 - n^{-6} - (k-1)e^{-\ln^3 n})(1 - e^{-\ln^3 n}) \ \ge \ 1 - n^{-6} - k \cdot e^{-\ln^3 n}.
\end{aligned}$$

□

5.5.3 Proof of Latency Lower Bound

We are now prepared to restate and prove Theorem 5.8.

Theorem 5.8. *Given a memoryless protocol $\mathcal{D}$, error probability $q(n) = 1/2$ or $q(n) = n^{-2}$, and constants $\beta \geq 10, \eta \stackrel{\text{def}}{=} p(1) > 0$, if $L_{\mathcal{D}}(n, q(n)) = o(n \log^{\beta/2-1} n)$, then for all sufficiently large n,*

$$\tilde{T}_{\mathcal{D}}(n) \geq \left\lfloor \frac{n(s^{\text{low}_\beta}(\lfloor n/\ln^2 n \rfloor) - s^{\text{low}_\beta}(\lfloor \sqrt{n} \rfloor))}{40\beta \ln\ln n} \right\rfloor.$$

Proof. Since $L_{\mathcal{D}}(n, q(n)) = o(n \log^{\beta/2-1} n)$, $s(\lfloor n/\ln^2 n \rfloor) \leq \frac{40 \ln n}{n} L_{\mathcal{D}}(n, q(n)) = o(\log^{\beta/2} n)$ by Lemma 5.5. It follows that $s(n^2) = o(\log^{\beta/2} n^2) = o(\log^{\beta/2} n)$.

Now let $\mathcal{A}$ be the adversary constructed by Theorem 5.7 with $\gamma = 5\beta$ and

$$T = \left\lfloor \frac{n(s^{\text{low}_\beta}(\lfloor n/\ln^2 n \rfloor) - s^{\text{low}_\beta}(\lfloor \sqrt{n} \rfloor))}{40\beta \ln\ln n} \right\rfloor \leq n^2.$$

Then $\mathcal{A}$ and T meet the requirements in Lemma 5.16. Consider a party u^* activated at time 0. For any time $t \in [1, T]$, if $\sigma^{\text{low}_\beta^{(\geq m)}}[t] \geq 4\beta \ln\ln n$, then the probability that u^* succeeds at time t is at most $p(t)e^{-4\beta \ln\ln n} = \frac{p(t)}{\ln^{4\beta} n}$. By Lemma 5.16, $\sigma^{\text{low}_\beta^{(\geq m)}}[t] \geq 4\beta \ln\ln n$ holds with probability at least $1 - 2n^{-6}$ for all $t \in [\lfloor n/\ln^2 n \rfloor, T]$. So the probability that u^* succeeds at time t is at most $\frac{p(t)}{\ln^{4\beta} n} + 2n^{-6}$ for all $t \in [\lfloor n/\ln^2 n \rfloor, T]$. For $[1, \lfloor n/\ln^2 n \rfloor)$, Lemma 5.4 implies that there are no successes in this interval with probability at least $1 - n^{-8}$. Thus, the expected number of u^*'s successes in $[1, T]$ is at most

$$\frac{\lfloor n/\ln^2 n \rfloor}{n^8} + \sum_{t=\lfloor n/\ln^2 n \rfloor}^{T} \left(\frac{p(t)}{\ln^{4\beta} n} + 2n^{-6} \right) \leq \frac{s(T)}{\ln^{4\beta} n} + 2n^{-4}.$$

By Markov's inequality, the probability that u^* succeeds in $[1, T]$ is at most

$$\frac{s(T)}{\ln^{4\beta} n} + 2n^{-4} \leq \frac{s(n^2)}{\ln^{4\beta} n} + 2n^{-4} = \frac{o(\ln^{\beta/2} n)}{\ln^{4\beta} n} + 2n^{-4} = o(1).$$

According to the definition of $\tilde{T}_{\mathcal{D}}(n)$, we have $\tilde{T}_{\mathcal{D}}(n) \geq T$ when n is sufficiently large. □

6 Upper Bounds in the LocalClock Model

In order to simplify the analysis of Contention Resolution protocols, we reduce the problem to analyzing the length of a *counter game*, for which the optimal adversarial strategy is obvious. In Section 6.1, we bound the time of a counter game in terms of its parameters. In Section 6.2, we apply this reduction to bound the latency of Contention Resolution protocols under the metrics *in expectation* and *with high probability*.

At a high level, we fix a special party u^* and aim to evaluate its latency. For both expected latency and high-probability latency, we design a protocol and select an interval $[a, a+r)$, where $a \geq t_{u^*}$ and $r \geq n$. Our goal is to show that the probability that u^* succeeds within this interval, conditioned on the event that it has not succeeded before time a, is either at least a constant (in the case of expected latency) or at least $1 - n^{-2}$ (in the case of high-probability latency). For a specific time slot $t \in [a, a+r)$, we focus on the quantity $\sigma[t] = \sum_{u \in A[t]} p(t - t_u)$, which represents the aggregate contention of the remaining parties at global time t. We consider the following three cases:

Low Contention. $\sigma[t] \leq 1$: In this case, party u^* succeeds with probability at least $p(t - t_{u^*})/4$, by Lemma 3.1.

Medium Contention. $1 < \sigma[t] \leq \frac{1}{4} \log_2 \log_2 n$: There is a non-negligible probability that at least one party succeeds.

High Contention. $\sigma[t] > \frac{1}{4} \log_2 \log_2 n$: This case cannot occur too many times, since the total sum of $\sigma[t]$ over the interval is bounded.

Rather than analyze the *actual* dynamics of σ over time, we effectively allow the adversary to *choose* the value of $\sigma[t]$ in each time step, subject to some budget constraints, which can be modeled directly as a counter game; see Definition 6.1.

6.1 Counter Games

Definition 6.1 (Counter Game)**.** The game is defined by

Parameters. Let $r, k, n_1, \ldots, n_{k-1}$ be positive integers and $c, \gamma_1, \ldots, \gamma_{k-1}$ be positive reals such that each $\gamma_i \in [c/r, 1]$.

Initialization. In the beginning $n'_i \leftarrow n_i$, for each $i \in \{1, \ldots, k-1\}$.

Game Play. In each round, based on the state $(n'_1, \ldots, n'_{k-1})$ the adversary plays some option $j \in [k]$.

When $j \in \{1, \ldots, k-1\}$: With probability γ_j, set $n'_j \leftarrow n'_j - 1$. If $n'_j < 0$ the game ends.

When $j = k$: With probability c/r the game ends.

Winning. The adversary wins if the game lasts at least r rounds.

In a counter game, the adversary's optimal strategy is clear: play options $j \in [k-1]$ until the first $k-1$ counters are reduced to zero, then play the option with the smallest probability of ending the game, which is always $j = k$ in the cases we consider.

Theorem 6.1. *Fix any adversarial strategy and let $\mathcal{E}^*$ be the event that the adversary wins, i.e., the game lasts at least r rounds. Then*

$$\Pr[\mathcal{E}^*] \leq \alpha + e^{-c(1-\frac{2}{r}\beta)},$$

where $\alpha = \sum_i e^{-n_i/6}$ and $\beta = \sum_i \frac{n_i}{\gamma_i}$.

Proof. For each $j \in [k-1]$, let $\mathcal{E}_j$ be the event that the adversary plays option j at least $2n_j/\gamma_j$ times and survives. The expected number of decrements to counter n'_j is at least $2n_j$, so we can upper bound $\Pr[\mathcal{E}_j] \le e^{n_j/6}$ using a standard Chernoff bound; see Appendix B.

Define $\mathcal{E}_k$ as the event in which the adversary plays option k at least $r - 2\beta$ times and survives. We have

$$\Pr[\mathcal{E}_k] = (1 - c/r)^{r-2\beta} \le e^{-c(1-\frac{2}{r}\beta)}.$$

Observe that if the adversary survives r rounds, at least one of the events $\mathcal{E}_1, \ldots, \mathcal{E}_k$ must occur. By a union bound,

$$\Pr[\mathcal{E}^*] \le \Pr[\mathcal{E}_1 \cup \cdots \cup \mathcal{E}_k] \le \sum_{j=1}^{k} \Pr[E_j] \le e^{-c(1-\frac{2}{r}\beta)} + \alpha.$$

□

6.2 Upper Bounds for Expected Latency and High-probability Latency

Theorem 6.1 allows us to bound the probability that a party executing a Contention Resolution protocol is unsuccessful for a period of time. We construct a memoryless protocol $\mathcal{D}$ to achieve the desired upper bound. Recall that $p(t - t_u)$ is the probability that an active party u grabs the resource at local time $t - t_u$, independent of the history.

Lemma 6.2. *Fix a memoryless protocol $\mathcal{D}$ and party $u^* \in [n]$. Define $\mathcal{E}(u^*, t)$ to be the event that u^* has yet to achieve success by global time t. Then*

$$\Pr\left[\mathcal{E}(u^*, a+r) \mid \mathcal{E}(u^*, a)\right] \le \exp\left(-c\left(1 - \frac{8n(\sqrt{\log_2 n} + U)}{r \log_2 \log_2 n}\right)\right) + n^{-20},$$

where $t_{u^*} \le a$, $p(j) \le 1/2$ for all j, $\sum_{j \in I} p(j) \le U$ for any interval I of length r, and $p(j) \ge \frac{4c}{r}$ for all $t \in [a, a+r)$.

Proof. Let $\sigma[t] = \sum_{u \in A[t]} p(t - t_u)$ be the aggregate contention at global time t. Each time slot $t \in [a, a+r)$ falls into one of the following three cases.

Case 1: $\sigma[t] \le 1$. By Lemma 3.1, u^* succeeds at time t with probability at least $p(t - t_{u^*})4^{-\sigma[t]} \ge \frac{c}{r}$.

Case 2: $1 < \sigma[t] \le \frac{1}{4}\log_2 \log_2 n$. Then the probability that *some* party succeeds at time t is at least $\sigma[t]4^{-\sigma[t]} \ge \frac{\frac{1}{4}\log_2 \log_2 n}{\sqrt{\log_2 n}}$.

Case 3: $\sigma[t] \ge \frac{1}{4}\log_2 \log_2 n$. The probability of success may be negligible. By definition of U, $\sum_{t \in [a, a+r)} \sigma[t] \le nU$, so the *number* of times $t \in [a, a+r)$ in Case 3 is at most $\frac{nU}{\frac{1}{4}\log_2 \log_2 n}$.

We map this situation onto a counter game with the following parameters. There are $k = 3$ options per play (corresponding to cases 2, 3, 1, respectively) and the number of rounds is r; play

1 has initial counter $n_1 = n - 1$ and success probability $\gamma_1 = \frac{1}{4}\log_2\log_2 n/\sqrt{\log_2 n}$; play 2 has initial counter $n_2 = 4nU/\log_2\log_2 n$ and success probability $\gamma_2 = 1$; play 3 ends the game with probability c/r. Applying Theorem 6.1, we observe that

$$\alpha = e^{-n_1/6} + e^{-n_2/6} = \exp\left(-\Omega(n(1 + U/\log\log n))\right) \le n^{-20},$$
$$\beta = n_1/\gamma_1 + n_2/\gamma_2 = \frac{n(\sqrt{\log_2 n} + U)}{\frac{1}{4}\log_2\log_2 n}.$$

The probability that the adversary can survive r rounds of the counter game is

$$\alpha + e^{-c(1-2\beta/r)} \le \exp\left(-c\left(1 - \frac{8n(\sqrt{\log_2 n} + U)}{r\log_2\log_2 n}\right)\right) + n^{-20}.$$

This is also an upper bound on the probability that u^* fails to find a successful time slot in the interval $[a, a + r)$. By modeling this situation as a counter game, we are effectively letting the adversary *choose* the aggregate contention $\sigma[t]$ as it likes, subject to a couple of budget constraints. The aggregate contention summed over $[a, a + r)$ cannot exceed nU, and the number of successes when $\sigma[t] \in (1, \frac{1}{4}\log_2\log_2 n]$ cannot exceed $n - 1$, for otherwise u^* must have been successful. □

Let us now apply Lemma 6.2 to bound the latency of Contention Resolution protocols.

Theorem 6.3 (Restatement of Theorem 1.4, Part 1 and Part 2)**.** *There exists a memoryless acknowledgment-based Contention Resolution protocol $\mathcal{D}$ such that the expected latency $L^{\exp}_{\mathcal{D}}(n) = O(n\log n/\log\log n)$.*

Proof. The protocol $\mathcal{D}$ is defined by the probability function $p = p_{\mathcal{D}}$:

$$p(j) = \frac{1}{2^{\lceil\log_2\lceil 1 + j/10\rceil\rceil}} = \Theta(1/j) \in [0, 1/2].$$

We need to bound the expected latency for an arbitrary party $u^* \in [n]$, which, without loss of generality, is activated at time $t_{u^*} = 0$. Let x be any integer for which $2^x > 100n\log_2 n/\log_2\log_2 n$. Let a be the first position such that $p(a) = \frac{1}{2^x}$. Then $p(j) = \frac{1}{2^x}$ for all $j \in [a, a + 10 \cdot 2^x)$.

We apply Lemma 6.2 to the range $[a, a + r)$, where $r = 10 \cdot 2^x$. Since $p(j)$ is monotonically nonincreasing, we can set $U = \sum_{j=1}^{r} p(j) \le \sum_{j=1}^{r} \min(\frac{10}{j}, \frac{1}{2}) \le 10\log_2 r$. Since $p(j) \ge \frac{1}{2^x}$ for $j \in [a, a + r)$, we may set $c = \frac{10}{4}$. Recall that $\mathcal{E}(u^*, t)$ is the event that u^* has yet to achieve success by global time t. According to Lemma 6.2, we have:

$$\begin{aligned}
\Pr\left[\mathcal{E}(u^*, a + r) \mid \mathcal{E}(u^*, a)\right] &\le \exp\left(-c\left(1 - \frac{8n(\sqrt{\log_2 n} + U)}{r\log_2\log_2 n}\right)\right) + n^{-20} \\
&\le \exp\left(-\frac{10}{4}\left(1 - \frac{8n(\sqrt{\log_2 n} + 10\log_2 r)}{r\log_2\log_2 n}\right)\right) + n^{-20} \\
&\le \exp\left(-\frac{10}{4}\left(1 - \frac{90n\log_2 r/\log_2\log_2 n}{r}\right)\right) + n^{-20} \\
&\le \exp\left(-\frac{10}{4}\cdot\frac{9}{10}\right) + n^{-20} \le 0.2.
\end{aligned}$$

The second last inequality is due to $\frac{90n \log_2 r / \log_2 \log_2 n}{r} \leq \frac{1}{10}$ for sufficiently large n and $r > 1000n \log_2 n / \log_2 \log_2 n$.

We are now prepared to analyze the expected latency of the protocol. Let x_0 be the *minimum* value such that $2^{x_0} \geq 100n \log_2 n / \log_2 \log_2 n$, and l_x as the first time slot for which $p(l_x - t_{u^*}) = \frac{1}{2^x}$ Then u^*'s expected latency is

$$\begin{aligned}
\mathbb{E}\left[L^{(u^*)}_{\mathcal{D},\mathcal{A}}\right] &\leq \left(\sum_{1 \leq x' < x_0} 10 \cdot 2^{x'}\right) + \sum_{x \geq x_0} 10 \cdot 2^x \cdot \Pr\left[\mathcal{E}(u^*, l_x)\right] \\
&= O(2^{x_0}) + \sum_{x \geq x_0} 10 \cdot 2^x \Pr\left[\mathcal{E}(u^*, l_x)\right] \prod_{x_0 < x' \leq x} \Pr\left[\mathcal{E}(u^*, l_{x'}) \mid \mathcal{E}(u^*, l_{x'-1})\right] \\
&\leq O(2^{x_0}) + \sum_{x \geq x_0} 10 \cdot 2^x (0.2)^{x - x_0} \\
&\leq O(2^{x_0}) \leq O(n \log n / \log \log n).
\end{aligned}$$

□

The following theorem was first claimed in the extended abstract of De Marco and Stachowiak [DS17], and later proved by De Marco, Kowalski, and Stachowiak [DKS22b]. Here we provide an alternate proof that depends on Lemma 6.2's reduction to a counter game.

Theorem 6.4 (Cf. [DKS22b, DS17])**.** *There exists a memoryless Contention Resolution protocol that guarantees latency $O(n \log^2 n / \log \log n)$ with high probability.*

Proof. The protocol is defined by the memoryless distribution $\mathcal{D}$, where

$$p(j) = \frac{\lceil \log_2 \lceil 1 + j/10 \rceil \rceil}{2^{\lceil \log_2 \lceil 1 + j/10 \rceil \rceil}} = \Theta(\log j / j) \in [0, 1/2],$$

for all $j \geq 1$. Let u^* be an arbitrary party.

Let x be any integer such that $2^x > 100n \log_2^2 n / \log_2 \log_2 n$. Let a be the first position with $p(a - t_{u^*}) = \frac{x}{2^x}$, and $r = 10 \cdot 2^x$. We will apply Lemma 6.2 to the interval $[a, a + r)$. Since $p(j)$ is monotonically non-increasing for integer $j \geq 1$, we can set

$$U = \sum_{j=1}^{r} p(j) \leq \sum_{x=1}^{\lceil \log_2 \lceil 1 + r/10 \rceil \rceil} \frac{x}{2^x} \cdot 10 \cdot 2^x \leq 10 \log_2^2 r.$$

To conform to the requirements of Lemma 6.2, we set $c = \frac{10x}{4}$ so that $p(j) = \frac{x}{2^x} = \frac{4c}{r}$. Now applying Lemma 6.2, we have

$$\begin{aligned}
\Pr\left[\mathcal{E}(u^*, a+r)\right] &= \Pr\left[\mathcal{E}(u^*, a)\right] \cdot \Pr\left[\mathcal{E}(u^*, a+r) \mid \mathcal{E}(u^*, a)\right] \\
&\leq \exp\left(-c\left(1 - \frac{8n(\sqrt{\log_2 n} + U)}{r \log_2 \log_2 n}\right)\right) + n^{-20} \\
&\leq \exp\left(-\frac{10x}{4}\left(1 - \frac{90n \log_2^2 r / \log_2 \log_2 n}{r}\right)\right) + n^{-20} \\
&\leq \exp\left(-\tfrac{10x}{4}\tfrac{9}{10}\right) + n^{-20} \\
&= \exp\left(-\tfrac{9}{4}\log_2\lceil 1 + r/10\rceil\right) + n^{-20} \\
&\leq \exp(-2\ln n) = n^{-2}.
\end{aligned}$$

□

7 Conclusion and Open Problems

The first contribution of this paper is to explore the power of the GlobalClock model for solving randomized Contention Resolution, in which parties perceive both the global clock and their local time since wake-up. We proved that GlobalClock is strictly stronger than LocalClock by exhibiting an *Elias code*-based protocol that achieves near-linear latency

$$O(n\zeta(4\log\log n)) = O(n \log\log n \log^{(3)} n \cdots 2^{O(\log^* n)}) = n(\log\log n)^{1+o(1)}.$$

The most pressing question is now to prove or disprove Conjecture 1.3(1), i.e., whether there exists a GlobalClock protocol with $O(n)$ latency, as well as its analogues Conjecture 1.3(2,3) for the unbounded setting.

In the LocalClock model we established sharp bounds on the latency of memoryless protocols under both the In-Expectation and With-High-Probability objectives, and also proved that optimality under both objectives cannot be achieved simultaneously. We believe the memoryless assumption is not critical, and that all of our lower bounds can be extended to arbitrary acknowledgment-based protocols. It is well known that proving lower bounds for acknowledgment-based protocols is more difficult [GL25, DS17, DKS22b], despite there being no obvious advantage to techniques that violate memorylessness.

References

[AHU74] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The design and analysis of computer algorithms.* Addison-Wesley, Reading, MA, 1974.

[Ald87] David J. Aldous. Ultimate instability of exponential back-off protocol for acknowledgment-based transmission control of random access communication channels. *IEEE Trans. Information Theory*, 33(2):219–223, 1987.

[AMM13] Antonio Fernández Anta, Miguel A. Mosteiro, and Jorge Ramón Muñoz. Unbounded contention resolution in multiple-access channels. *Algorithmica*, 67(3):295–314, 2013.

[BFG06] Michael A. Bender, Jeremy T. Fineman, and Seth Gilbert. Contention resolution with heterogeneous job sizes. In *Proceedings 14th Annual European Symposium on Algorithms (ESA)*, pages 112–123, 2006.

[BFG+24] Michael A. Bender, Jeremy T. Fineman, Seth Gilbert, John Kuszmaul, and Maxwell Young. Fully energy-efficient randomized backoff: Slow feedback loops yield fast contention resolution. In *Proceedings of the 43rd ACM Symposium on Principles of Distributed Computing (PODC)*, pages 231–242, 2024.

[BFGY19] Michael A. Bender, Jeremy T. Fineman, Seth Gilbert, and Maxwell Young. Scaling exponential backoff: Constant throughput, polylogarithmic channel-access attempts, and robustness. *J. ACM*, 66(1):6:1–6:33, 2019.

[BFH+04] Michael A. Bender, Martin Farach-Colton, Simai He, Bradley C. Kuszmaul, and Charles E. Leiserson. Adversarial analyses of window backoff strategies. In *Proceedings 18th International Parallel and Distributed Processing Symposium (IPDPS)*, 2004.

[BFH+05] Michael A. Bender, Martin Farach-Colton, Simai He, Bradley C. Kuszmaul, and Charles E. Leiserson. Adversarial contention resolution for simple channels. In *Proceedings of the 17th Annual ACM Symposium on Parallelism in Algorithms and Architectures (SPAA)*, pages 325–332, 2005.

[BKKP20] Michael A. Bender, Tsvi Kopelowitz, William Kuszmaul, and Seth Pettie. Contention resolution without collision detection. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 105–118, 2020.

[BKPY18] Michael A. Bender, Tsvi Kopelowitz, Seth Pettie, and Maxwell Young. Contention resolution with constant throughput and log-logstar channel accesses. *SIAM J. Comput.*, 47(5):1735–1754, 2018.

[Cap79] John Capetanakis. Tree algorithms for packet broadcast channels. *IEEE Trans. Information Theory*, 25(5):505–515, 1979.

[CGKR05] Bogdan S. Chlebus, Leszek Gasieniec, Dariusz R. Kowalski, and Tomasz Radzik. On the wake-up problem in radio networks. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP)*, volume 3580 of *Lecture Notes in Computer Science*, pages 347–359, 2005.

[CJP19] Yi-Jun Chang, Wenyu Jin, and Seth Pettie. Simple contention resolution via multiplicative weight updates. In *Proceedings of the 2nd Symposium on Simplicity in Algorithms, (SOSA)*, volume 69 of *OASIcs*, pages 16:1–16:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[CLRS22] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, 4th ed.* MIT Press, 2022.

[CMS01] Andrea E. F. Clementi, Angelo Monti, and Riccardo Silvestri. Distributed multibroadcast in unknown radio networks. In *Proceedings of the 20th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 255–264, 2001.

[DK15] Gianluca De Marco and Dariusz R. Kowalski. Fast nonadaptive deterministic algorithm for conflict resolution in a dynamic multiple-access channel. *SIAM J. Comput.*, 44(3):868–888, 2015.

[DKS22a] Gianluca De Marco, Dariusz R. Kowalski, and Grzegorz Stachowiak. Contention resolution without collision detection: Constant throughput and logarithmic energy. In *Proceedings of the 36th International Symposium on Distributed Computing (DISC)*, volume 246 of *LIPIcs*, pages 17:1–17:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[DKS22b] Gianluca De Marco, Dariusz R. Kowalski, and Grzegorz Stachowiak. Time and energy efficient contention resolution in asynchronous shared channels. *CoRR*, abs/2209.14140, 2022.

[DP09] Devdatt P. Dubhashi and Alessandro Panconesi. *Concentration of Measure for the Analysis of Randomized Algorithms*. Cambridge University Press, 2009.

[DPV06] Sanjoy Dasgupta, Christos H. Papadimitriou, and Umesh V. Vazirani. *Algorithms*. McGraw-Hill, 2006.

[DS17] Gianluca De Marco and Grzegorz Stachowiak. Asynchronous shared channel. In *Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC)*, pages 391–400, 2017.

[Eli75] Peter Elias. Universal codeword sets and representations of the integers. *IEEE Transactions on Information Theory*, 21(2):194–203, 1975.

[Gal78] Robert G. Gallager. Conflict resolution in random access broadcast networks. In *Proceedings AFOSR Workshop on Communications Theory Applications, Provincetown, MA, Sept 17–20*, pages 74–76, 1978.

[GFL87] Albert G. Greenberg, Philippe Flajolet, and Richard E. Ladner. Estimating the multiplicities of conflicts to speed their resolution in multiple access channels. *J. ACM*, 34(2):289–325, 1987.

[GL25] Leslie Ann Goldberg and John Lapinskas. Instability of backoff protocols with arbitrary arrival rates. *J. Comput. Syst. Sci.*, 152:103638, 2025.

[HL14] Godfrey H. Hardy and John E. Littlewood. Some problems of Diophantine approximation. *Acta Mathematica*, 37:155–238, 1914.

[KET05] Jon Kleinberg and Éva Tardos. *Algorithm Design*. Addison-Wesley, Boston, MA, 2005.

[KG85] János Komlós and Albert G. Greenberg. An asymptotically nonadaptive algorithm for conflict resolution in multiple-access channels. *IEEE Transactions on Information Theory*, 31(2):302–306, 1985.

[Kha89] L. S. Khasin. Conflict resolution in a multiple access channel. *Probl. Peredachi Inf. (Problems Inform. Transmission)*, 25(4):63–68, 1989.

[Knu76] Donald E. Knuth. Big Omicron and Big Omega and Big Theta. *SIGACT News*, April-June:18–24, 1976.

[MH85] Jeannine Mosely and Pierre A. Humblet. A class of efficient contention resolution algorithms for multiple access channels. *IEEE Trans. Communications*, 33(2):145–151, 1985.

[MT81] V. A. Mikhailov and B. S. Tsybakov. Upper bound for the capacity of a random multiple access system. *Problemy Peredachi Informatsii*, 17(1):90–95, 1981.

[TM78] B. S. Tsybakov and V. A. Mikhailov. Slotted multiaccess packet broadcasting feedback channel. *Problemy Peredachi Informatsii*, 14(4):32–59, 1978.

A Asymptotic Notation: The Definition of Ω

Is saying g cannot be $o(f)$ the same as saying $g = \Omega(f)$? This goes back to a minor controversy of the 1970s on the proper definition of asymptotic notation for non-negative $\mathbb{Z}^+ \to \mathbb{R}^+$ functions, particularly the definition of Ω. Everyone agreed that $g = O(f)$ means $g(n) \leq cf(n)$ for some $c > 0$ and all sufficiently large n. Aho, Hopcroft, and Ullman's 1974 text [AHU74] defined Ω as:

$$g = \Omega_{\text{AHU}}(f) \text{ if } g(n) \geq cf(n) \text{ for some } c > 0 \text{ and } \textit{infinitely many } n.$$

In 1976 Knuth [Knu76] published a history of asymptotic notation and dated the Aho-Hopcroft-Ullman definition of Ω to a 1914 paper of Hardy and Littlewood [HL14]. Without advancing a specific argument, Knuth [Knu76] stated that a definition of Ω symmetric to O would prove to be most useful for computer scientists, namely

$$g = \Omega_{\text{K}}(f) \text{ if } g(n) \geq cf(n) \text{ for some } c > 0 \text{ and all sufficiently large } n.$$

Although Knuth's definition Ω_{K} is most common in today's textbooks [CLRS22, KET05, DPV06], most computer scientists operationally use Ω to mean either Ω_{AHU} or Ω_{K}, depending on context.

The problem, as Aho, Hopcroft, and Ullman discussed [AHU74], is that some problems are not expected to be uniformly and simultaneously hard for all values of n. This is certainly true in Contention Resolution, where approximating "n" is the crux of the problem. For example, De Marco, Kowalski, and Stachowiak [DKS22b] assert a lower bound of $\Omega(n \log n/(\log\log n)^2)$, *by which they mean* $\Omega_{\text{AHU}}(n \log n/(\log\log n)^2)$. It is perfectly consistent with [DKS22b] and our lower bounds that there is a Contention Resolution scheme with latency, say, $O(n \log\log\log n)$ whenever n is of the form $2^{2^{2^{2^k}}}$, making it essentially impossible to say something meaningful using Knuth's Ω_{K} notation.

In our view, when describing the asymptotic complexity of problems, Ω_{AHU} is more attractive than Ω_{K}. It is nearly always more useful for "Ω" to be the logical negation of "o" than the logical converse of "O."

B Tail Bounds

Lemma B.1 (Classical Azuma-Hoeffding Bound, see e.g. [DP09])**.** *Let $X_1, \ldots, X_n$ be independent random variables such that $X_i \in [a_i, b_i]$ almost surely. Let $\mu = \sum_{i=1}^n \mathbb{E}[X_i]$, then for any $\epsilon > 0$,*

$$\Pr\left[\left(\sum_{i=1}^n X_i\right) \geq (1+\epsilon)\mu\right], \Pr\left[\left(\sum_{i=1}^n X_i\right) \leq (1-\epsilon)\mu\right] \leq \exp\left(-\frac{2\epsilon^2\mu^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

Lemma B.2 (Chernoff Bound)**.** *Let $X_1, \ldots, X_n$ be independent random variables with range $[0, v]$. Let $\mu = \sum_{i=1}^{n} \mathbb{E}[X_i]$, then for all $\epsilon > 0$,*

1. $\Pr\left[\left(\sum_{i=1}^{n} X_i\right) \geq (1+\epsilon)\mu\right] \leq \left(\frac{e^{\epsilon}}{(1+\epsilon)^{1+\epsilon}}\right)^{\mu/v}$
2. $\Pr\left[\left(\sum_{i=1}^{n} X_i\right) \leq (1-\epsilon)\mu\right] \leq \left(\frac{e^{-\epsilon}}{(1-\epsilon)^{1-\epsilon}}\right)^{\mu/v}$

Corollary B.3. *Let $X_1, \ldots, X_n$ be independent random variables supported on $[0, v]$, and let $\mu = \sum_{i=1}^{n} \mathbb{E}[X_i]$. Then the following inequalities hold:*

1. $\Pr\left[\sum_{i=1}^{n} X_i \geq 2\mu\right] \leq \exp\left(-\frac{\mu}{3v}\right)$,
2. $\Pr\left[\sum_{i=1}^{n} X_i \leq \mu/2\right] \leq \exp\left(-\frac{\mu}{7v}\right)$.

Proof.
Proof of Part 1. Applying Lemma B.2 (i) with $\epsilon = 1$, we obtain

$$\left(\frac{e^{\epsilon}}{(1+\epsilon)^{1+\epsilon}}\right)^{\mu/v} = \left(\frac{e}{2^2}\right)^{\mu/v} \leq e^{-\mu/(3v)}.$$

Proof of Part 2. Applying Lemma B.2 (ii) with $\epsilon = 1/2$, we obtain

$$\left(\frac{e^{-\epsilon}}{(1-\epsilon)^{1-\epsilon}}\right)^{\mu/v} = \left(\frac{e^{-1/2}}{(1/2)^{1/2}}\right)^{\mu/v} \leq e^{-\mu/(7v)}.$$

□

C Omitted Proofs

C.1 Proof of Lemma 3.1

Let us recall the two claims of Lemma 3.1. For a global time t, $p_u = \Pr\left[X_{t-t_u}^{(u)} = 1\right]$ is the probability that u grabs the shared resource and $\sigma = \sigma[t] = \sum_{u \in A[t]} p_u$.

1. If $p_u \in [0, 1/2]$ for all $u \in A[t]$, then $\Pr\left[\left(\sum_{u \in A[t]} X_{t-t_u}^{(u)}\right) = 1\right] \geq \sigma 4^{-\sigma}$, and u's probability of success is at least $p_u 4^{-\sigma}$.
2. $\Pr\left[\left(\sum_{u \in A[t]} X_{t-t_u}^{(u)}\right) = 1\right] \leq \sigma e^{-\sigma+1}$ and $\Pr\left[\left(\sum_{u \in A[t]} X_{t-t_u}^{(u)}\right) \leq 1\right] \leq e^{-\sigma} + \sigma e^{-\sigma+1}$.

Proof of Lemma 3.1.
Part 1. We use the approximation $(1-x) \geq 4^{-x}$ for $x \in [0, 1/2]$. The probability of success is:

$$\Pr\left[\left(\sum_{u \in A[t]} X_{t-t_u}^{(u)}\right) = 1\right] = \sum_{u \in A[t]} p_u \prod_{v \in A[t]-\{u\}} (1-p_v) \geq \sigma 4^{-\sigma}.$$

Moreover, u's probability of success is $p_u \prod_{v \in A[t]-\{u\}}(1-p_v) \geq p_u 4^{-\sigma}$.

Part 2. We know $1 - x \leq e^{-x}$ for any x, so

$$\Pr\left[\left(\sum_{u \in A[t]} X_{t-t_u}^{(u)}\right) = 1\right] = \sum_{u \in A[t]} p_u \prod_{v \in A[t]\setminus\{u\}} (1-p_v) \leq \sigma e^{-\sigma+1},$$
$$\Pr\left[\left(\sum_{u \in A[t]} X_{t-t_u}^{(u)}\right) = 0\right] = \sum_{u \in A[t]} (1-p_u) \leq e^{-\sigma}.$$

□

Note that when $\sigma \geq 2$, it is impossible to get a non-zero lower bound on the probability of success without imposing some non-trivial upper bound on the probabilities, such as $p_i \in [0, 1/2]$.

C.2 Proof of Lemma 5.10(v)

Lemma C.1 and Corollary C.2 prove part (v) of Lemma 5.10.

Lemma C.1. *Suppose $f(n)$ is nonnegative, monotone nondecreasing and $f(n+1) - f(n) \leq f(n+1)/2$ when $n \geq n_0$. Fix some $0 \leq c < 1$ and integer $n \geq n_0$. Let n' be the largest integer such that $f(n') \leq cf(n)$. If $f(n_0) \leq c \cdot f(n)$, then $f(n') \geq cf(n)/2$.*

Proof. Since $f(n_0) \leq cf(n)$, $n' \geq n_0$. By the definition of n', we have $f(n'+1) > cf(n)$. So

$$f(n') = f(n'+1) - (f(n'+1) - f(n')) \geq f(n'+1)/2 > cf(n)/2.$$

□

Corollary C.2. *Let $q(n)$ be either $q(n) = 1/2$ or $q(n) = n^{-2}$, and recall that $U(n) = \lfloor \frac{n \ln(1/q(n)) \ln n}{\ln \ln n} \rfloor$. For sufficiently large n and a real number $c \in [20/n, 1)$, let n' be the largest integer such that $U(n') \leq cU(n)$. Then*

$$U(n') \geq cU(n)/2.$$

Proof. Clearly $U(n+1) - U(n) = O(\frac{\ln(1/q(n)) \ln n}{\ln \ln n}) \leq U(n+1)/2$ and $U(n)$ is monotone increasing when n is large, say $n \geq n_0$. Since $c \geq 20/n$, $cU(n) = \Omega(\frac{\ln(1/q(n)) \ln n}{\ln \ln n}) \geq U(n_0)$ for sufficiently large n. The conclusion follows from Lemma C.1. □