Credible, Truthful, and Bounded-Round Mechanisms via Cryptographic Commitments

MATHEUS V. X. FERREIRA, Princeton University
S. MATTHEW WEINBERG, Princeton University

We consider the sale of a single item to multiple buyers by a revenue-maximizing seller. Recent work of Akbarpour and Li formalizes *credibility* as an auction desideratum, and prove that the only optimal, credible, strategyproof auction is the ascending price auction [AL19].

In contrast, when buyer valuations are MHR, we show that the mild additional assumption of a cryptographically secure commitment scheme suffices for a simple *two-round* auction which is optimal, credible, and strategyproof.

We extend our analysis to the case when buyer valuations are α-strongly regular for any $\alpha > 0$, up to arbitrary ε in credibility. Interestingly, we also prove that this construction cannot be extended to regular distributions, nor can the ε be removed with multiple bidders.

Additional Key Words and Phrases: Credible Mechanisms; Cryptographic Auctions; Optimal Auction Design; Mechanism Design and Approximation; Mechanism Design with Imperfect Commitment.

1 INTRODUCTION

We consider a revenue-maximizing auctioneer with a single item to sell to multiple bidders. Starting from Myerson's seminal work, it is traditionally assumed that the seller can commit to an auction format but that buyers must be incentivized to report their true values. Several recent works have moved beyond this assumption in repeated auctions, for example, where sellers can commit to a particular auction *today*, but not to their behavior *tomorrow* (e.g., [DPS14, ILPT17, LMSZ19]). Even more recent work of Akbarpour and Li proposes a framework also for one-shot auctions [AL19]. Our paper fits within this later framework.

Specifically, each buyer i's value v_i for the item is drawn independently from a distribution D_i, and the seller knows these distributions but not the precise values. As in [Mye81], we seek auctions which are incentive compatible, and optimal among all incentive compatible auctions. [AL19] introduces a new desideratum, *credibility*. Informally, an auction is credible if the auctioneer themselves is incentivized to execute the auction in earnest, even when permitted to cheat in ways that are undetectable to the bidders (see Section 2 for a formal definition in single-item auctions).

Akbarpour and Li prove a comprehensive trilemma for single-item auctions: Myerson's auction is the unique truthful, one-round, revenue-maximizing auction, but it is not credible. Moreover, the ascending-price auction is the unique truthful, revenue-maximizing, credible auction, but it requires an unbounded number of rounds. Finally, the first-price auction is the unique revenue-maximizing, credible, one-round auction, but it is not truthful.

Classical auction theory might take truthfulness as a first-order concern, and view the tradeoff between bounded-round and credibility as second-order. But as more and more auctions are run online, credibility is not just a "bonus feature", but a serious consideration. Specifically, reserve price-setting in ad auctions is often opaque, and a desire for transparency in execution has led major ad exchanges to switch from truthful second-price auctions to non-truthful (but credible) first-price auctions [Kle02, Slu19]. At the same time, these auctions are executed in milliseconds and must conclude before a search browser loads, so bounding the number of rounds is now a first-order concern as well.

In this context, the trilemma of [AL19] may feel like a negative result: it is impossible to achieve all three first-order desiderata at once. Our main result circumvents their trilemma and provides a truthful, revenue-maximizing, credible, two-round auction, *under the assumption of basic cryptographic primitives*. That is, viewed through the framework of [AL19] verbatim, our auctions are not credible (see Section 4 for an example). But, provably, no auctioneer can find a profitable deviation without breaking standard cryptographic assumptions.

Interestingly, our construction is not a magic bullet with a trivial proof — we must still carefully reason about the incentives of the auctioneer within our framework. Informally, our main results are (all under the assumption of a cryptographically secure commitment scheme, see Section 2 for formal assumption, and also for formal definitions of distribution classes):

- When all D_i are MHR, there is a truthful, revenue-maximizing, credible, two-round auction (Theorem 4.1).
- When all D_i are α-strongly regular for any $\alpha \in (0,1)$, there is a truthful, revenue-maximizing, ε-credible, two-round auction (Theorem 4.2).
- When there is a single bidder whose distribution is α-strongly regular for any $\alpha \in (0,1)$, there is a truthful, revenue-maximizing, credible, two-round auction (Proposition 4.1).
- This auction is *not* necessarily credible when there is a single buyer from a regular distribution, so extensions to regular distributions are not possible (Theorem 4.3).
- For any $\alpha \in (0,1)$, this auction is *not* necessarily credible when all D_i are α-strongly regular, so the ε is necessary in bullet two (Theorem 4.4).

1.1 Brief Technical Overview

Our auctions are still fairly simple and require only the basic cryptographic primitive of *commitment schemes*. Informally, a commitment scheme allows a sender to send a *commitment* c_i to a bid b_i, such that any user who sees only c_i learns absolutely nothing about b_i. Moreover, the sender can later *reveal* b_i, in a way that proves they committed to b_i in the first place (assuming the sender is computationally bounded). So our skeleton is simply to (a) ask each bidder to commit to their bid, (b) forward these commitments to all other bidders, (c) ask each bidder to reveal, (d) forward these revealed bids to all other bidders. We formalize this strawman auction in Section 3.

The outlook for this strawman auction initially looks promising: it is truthful, revenue-optimal, and two-round. Like in the auctions considered in [AL19], the primary way in which the auctioneer can deviate is by submitting fake bids. It is not too hard to argue that *if the auctioneer must reveal all committed bids*, then there is no way the auctioneer can deviate from being honest in a way that is both undetectable and profitable. However, the auction must have a well-defined execution even if some bids are *concealed* (that is, the committed bid is never revealed). Should the auction simply stall? If so, it is undoubtedly in the auctioneer's interest to reveal all bids. Still, this auction is extremely not robust to latency, or an adversarial attack (simply commit a bid and disappear). Perhaps the auction should reboot? This also seems undesirable, as now the auctioneer has learned some private information.

A natural suggestion (implemented in the strawman auction) is instead to replace all missing bids with 0. This change, however, now gives the auctioneer a new class of potential deviations: they can commit to many different fake bids and reveal them selectively based on the true bids. It is not hard to see that this auction is not credible.

We propose a straightforward modification, which is to fine any bidder who commits but does not reveal, *and pay this fine to the winning bidder*. Now, the auctioneer faces a tradeoff: they can still commit to as many fake bids as they like, and they can still selectively reveal them. But for every bid they choose to conceal, they pay a fine. The entire technical portion of this paper is understanding when a sufficiently large fine exists to disincentivize the auctioneer from cheating in this particular way, and how large this fine must be. The bullet points above summarize our findings: such fines exist when all distributions are MHR, and (almost) exist when all distributions are α-strongly regular, but do not necessarily exist even with one buyer from a regular distribution.

1.2 Related Work

We have already overviewed the most related work above: we work in the model proposed by [AL19], additionally with cryptographic primitives. There is a substantial literature generally on secure multi-party computation since Yao's millionaire problem [Yao82] (see chapter 7 of [Gol09] for a survey on the topic), most of which is unrelated to our paper.

The easiest distinction between (most of) these works and ours is that they are not *Sybil-proof*. Specifically, there is some trusted setup where every participant has an identity. Results such as [NS93] replace commitments with strong public-key infrastructure in our strawman proposal. Specifically, such protocols assume that a *majority of participants* are honestly following the protocol. In online auctions, there is no hope of preventing the auctioneer from creating thousands of fake bidders if it will (undetectably) increase their revenue (so while a majority of "real participants" may be honest, the "digital participants" are nearly-unanimously *not* following the protocol). A second distinction is that these protocols are often extremely complex, and certainly do not terminate in two rounds. Indeed, a central challenge for modern research in multi-party computation is developing practically reasonable protocols.

Our work is not the first to propose the use of fines to disincentivize participants from aborting a protocol [BPRP08, BK14], as there are known impossibility results (without monetary incentives) when participants can abort [Cle86].

1.3 Roadmap

Section 2 formalizes our problem of study, including cryptographic primitives. Section 3 analyzes the strawman auction as a warmup. Section 4 proposes our auction, proves some basic facts, and states our main results. Sections 5 through 7 prove our main results. All technical sections present intuition, along with proofs (although some technical lemmas are deferred to the appendix).

2 PRELIMINARIES

We first overview formalities with regards to auctions. Our model and definitions are identical to [AL19], but repeated for clarity and completeness.

2.1 Auctions

There is a single seller with a single indivisible item and n bidders. Each bidder i has a private value v_i for the item, which is drawn from a distribution D_i. We let $D := \times_i D_i$, and use $\mathrm{Rev}(D)$ to denote the expected revenue of the optimal auction when buyers are drawn from D.

Communication and rounds. The seller communicates with each bidder using a private channel (and this is the only communication — the bidders do not communicate with each other). In every round, the following occurs: (a) each bidder chooses a message to send to the auctioneer, (b) the auctioneer processes all received messages, (c) the auctioneer chooses a (personalized) message to send to each bidder. At any point, the auctioneer may terminate and select a winner of the item (potentially no one), and charge prices. Importantly, each bidder communicates only with the auctioneer, and learns only whether or not they win the item and how much they pay upon termination (if they lose, they do not learn who wins, nor how much the winner pays). We also assume there is a default message $\perp$, which is sent if the bidder stays silent during a round.

Game. Observe that the communication model induces an extended form game among the bidders and the auctioneer. Like [AL19], we are interested in the case where the auctioneer commits publicly to a strategy which terminates in finite rounds with probability 1. This induces an extended form game among the bidders. We'll refer to this game as the auction, and repeat the following definitions:

Definition 2.1 (Strategyproof/Ex-Post Nash/Individually Rational). *An auction is* strategyproof *if for all i there exists a mapping $s_i(\cdot)$ from values to strategies, and additionally for all i and all $\vec{v}$, $s_i(v_i)$ is a best response of bidder i to $\vec{s}_{-i}(\vec{v}_{-i})$. That is, for all $\vec{v}$, if the buyer valuations are $\vec{v}$, then $\langle s_1(v_1), \ldots, s_n(v_n)\rangle$ forms an ex-post Nash.*[1]

In this paper, we will only consider auctions for which there is a unique $s_1(\cdot), \ldots, s_n(\cdot)$ that always form an ex-post Nash, and refer to these strategies as "telling the truth."

An auction is individually rational *if telling the truth guarantees non-negative expected utility.*

Definition 2.2 (Safe Deviation). *A* safe deviation *for the auctioneer in the communication game is a strategy which does not necessarily implement the promised auction, but for every bidder i, their personal communication with the auctioneer and resulting allocation/price is consistent with some $\vec{s}_{-i}$.*

Definition 2.3 (Credible). *An auction is* credible *if, in expectation over $\vec{v} \leftarrow D$, and buyers being truthful, executing the auction in earnest maximizes expected revenue over all safe deviations.*

Example 2.1 (Second-Price Auction). *[AL19] establishes that the second-price auction is not credible. Consider when $v_1 = 5$ and $v_2 = 10$. An earnest execution of the second-price auction would give the item to bidder 2 and charge 5. However, the auctioneer could instead give bidder 2 the item and charge 9 — this is a safe deviation because it is consistent with buyer 1 bidding 9.*

2.2 Computational Assumptions and Basic Cryptography

The only difference between our model and that of [AL19] is that we consider computationally-bounded participants and the existence of basic cryptographic primitives. Let λ denote a security parameter (one should think of λ as some number in the hundreds: it is reasonable to assume that all participants can do computation which terminates in time poly(λ), but also that no participant can execute computation which terminates in time 2^{λ}).

Commitment Scheme. A commitment scheme is a function $\text{Commit}(\cdot, \cdot)$ which takes as input a message message m, a one-time pad r, and outputs a commitment c. We assume that a commitment scheme with the properties below exists for any desired λ. Informally, a scheme is computationally binding if once a sender commits to a message m with some r, they cannot find another message $m' \neq m$ and r' such that $\text{Commit}(m', r') = \text{Commit}(m, r)$. A scheme is perfectly hiding if the distribution of commitments produced on message m when r is uniformly random *is independent of m* (and therefore, even a computationally unbounded receiver learns nothing about m).

Assumption 2.1. *There exists a cryptographic commitment scheme satisfying:*

- *(Efficiency) The function Commit$(\cdot, \cdot)$ can be implemented in time poly$(\lambda, |m|, |r|)$.*
- *(Computationally Binding) For any algorithm A which takes as input a message m, terminates in expected time poly$(\lambda, |m|)$, and outputs r, m', r', and all messages m, A breaks commitment w.p. $\leq 2^{-\lambda}$. Formally:* $\Pr[\text{Commit}(m, r) = \text{Commit}(m', r'),\ \text{and } m \neq m'] \leq 2^{-\lambda}$.
- *(Perfectly Hiding) The distributions of Commit(m, r) and Commit(m', r'), when r, r' are uniformly random, are identical distributions for all m, m'.*
- *(Non-malleable) Formal definitions of non-malleability are quite involved and require multiple pages to formally state [DDN03, FF00]. Informally, non-malleability guarantees that any*

[1] In other words, an auction need not be direct-revelation in order to be strategyproof, but there must exist a strategy $(s_i(v_i))$ which bidder i can use which is akin to "reporting v_i."

commitment a computationally-bounded adversary could produce, upon receiving commitments $c_1, \dots, c_{poly(\lambda)}$, could also be produced without $c_1, \dots, c_{poly(\lambda)}$.

There are indeed commitment schemes which are believed to satisfy Assumption 2.1, such as the Pedersen scheme with digital signatures.[2] Note that the particular choice of a perfectly hiding (versus computationally hiding) scheme is not crucial for the spirit of our results. However, it does allow significantly cleaner theorem statements. Similarly, our main positive result (Theorem 4.1) doesn't require non-malleability, although it does make proofs cleaner (our main extension, Theorem 4.2 necessarily requires non-malleability). Informally, Assumption 2.1 implies that unless the auctioneer is relying on events which occur with probability at most $2^{-\lambda}$, or is computationally unbounded, the auctioneer cannot perform an *unreasonable deviation*, defined below.

Definition 2.4 (Reasonable Deviation). *Say that a commitment c is* explicitly tied to (m, r) *if the participant (bidder or auctioneer) who sent c explicitly computed $c := (m, r)$. A* reasonable deviation *for the auctioneer in the communication game is a strategy such that whenever the auctioneer reveals a commitment to c, with $c = Commit(m, r)$, c was explicitly tied to (m, r).*

Observe that one kind of unreasonable deviation would violate computational binding: the auctioneer might compute $c := \text{Commit}(m, r)$, but later reveal that $c := \text{Commit}(m', r')$ (unreasonable because c is explicitly tied to (m, r), not (m', r')). Another kind would violate non-malleability: the auctioneer might receive commitments $c_1 := \text{Commit}(m_1, r_1), c_2 := \text{Commit}(m_2, r_2)$ and send $c_3 := \text{Commit}(\max\{m_1, m_2\}, r_1 + r_2)$ without knowing m_1, m_2 (unreasonable because c_3 is not explicitly tied to anything).

Definition 2.5 (Computationally Credible). *An auction is* computationally credible *if, in expectation over $\vec{v} \leftarrow D$, and buyers being truthful, the auctioneer maximizes their expected revenue, over all deviations which are both safe and reasonable, by executing the auction in earnest.*

An auction is computationally ε-credible if executing the auction in earnest yields a $(1 - \varepsilon)$-fraction of the expected revenue of any safe, reasonable deviation.

Our main results will design auctions that are computationally credible (Theorem 4.1). One of our extensions will design an auction which is computationally ε-credible (Theorem 4.2), and some of our lower bounds rule out ε-credible mechanisms for ε arbitrarily close to one (Theorem 4.3).

Intuitively, what is convenient about perfect (versus computational) hiding, is that we get for free that the auctioneer learns *nothing* about bidders' commitments until they are revealed (with imperfect hiding, we only know that they learn very little, and perhaps this little bit of information could help them achieve a little bit more revenue). What is convenient about computational binding is that there is a discrete undesirable event (that anyone finds an $m \neq m'$ such that $\text{Commit}(m, r) = \text{Commit}(m', r')$), which occurs or doesn't occur. We can therefore cleanly separate executions where this event occurs (and separately observe that this event occurs with extremely low probability, due to computational binding and non-malleability), and those where they don't (and confirm that the auctioneer is *exactly* best-responding subject to this event not occurring).

[2] Briefly, the Pedersen scheme requires a group of prime order p under which the discrete logarithm is (believed to be) hard, with generator g. Every potential receiver of a message raises g to a random power to get another generator h, and publicly announces h. Then $\text{Commit}(m, r) := g^m \cdot h^r$. Observe that for all c and all m, there exists a unique r such that $g^m \cdot h^r = c$ (so the scheme is perfectly hiding). But if a sender were able to break their commitment, this would explicitly learn $\log_g(h)$, so it is also computationally binding. As stated, the scheme is malleable: an adversary could see $g^m h^r$ and multiply it by g^2 to now get $g^{m+2}h^r = \text{Commit}(m + 2, r)$. The scheme can be made non-malleable by first using any non-malleable digital signature scheme. Note that to use exactly the Pedersen commitment scheme (with digital signatures), every bidder i would need to share their own h_i in order to receive binding commitments (and a public key), which can be done in one additional preprocessing round, and this preprocessing round could be done once and reused across indefinitely-many auctions.

2.3 Virtual Values

For a continuous single-dimensional distribution with CDF F and PDF f, the *virtual value* of x is $\varphi^F(x) := x - \frac{1-F(x)}{f(x)}$. We also use $h^F(x) := \frac{f(x)}{1-F(x)}$ the *hazard rate* of F. We drop the superscript F if it is clear from context, and will use subscripts of i instead of superscripts of D_i (e.g. $h_i(x) := h^{D_i}(x)$). Note that virtual values and hazard rates are well-defined for discrete distributions as well, and satisfy all the same properties as virtual values for continuous distributions (see, e.g., [CDW19]).[3] For ease of exposition, we provide our examples and analysis on continuous distributions, which carries over verbatim to discrete distributions due to explicit limiting arguments provided in [CDW19, Section 4]. Seminal work of Myerson asserts that the expected revenue of any strategyproof mechanism is its expected virtual welfare.

Theorem 2.1 ([Mye81]). *Let a strategy proof mechanism award bidder i the item with probability $x_i(\vec{b})$ on bids $\vec{b}$, and charge them $p_i(\vec{b})$. Then:*

$$E_{\vec{v}\leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v})\right] = E_{\vec{v}\leftarrow D}\left[\sum_{i=1}^{n} x_i(\vec{v})\varphi_i(v_i)\right]$$

Finally, we conclude with a definition of classes of distributions which are relevant for our results.

Definition 2.6 (Regular, MHR, α-Strongly Regular). *A distribution F is α-*strongly regular *if for all $v' \geq v$, $\varphi^F(v') - \varphi^F(v) \geq \alpha(v' - v)$. A distribution is* regular *if it is 0-strongly regular, and* monotone hazard rate (MHR) *if it is 1-strongly regular.*

3 STRAWMAN COMPUTATIONALLY CREDIBLE AUCTIONS

We propose a simple modification to any direct revelation mechanism, which turns these one-round mechanisms into two-round mechanisms. In round one, the buyer's communication is simply a commitment to a bid. The auctioneer's communication is to forward these commitments to all bidders. In round two, the buyer's communication is to decommit (reveal their bid to the auctioneer). The auctioneer's communication is to forward all (decommitted) bids to the buyers. We use the terminology *reveal c_i* when a message (m_i, r_i) such that $\text{Commit}(m_i, r_i) = c_i$ is sent, and *conceal c_i* when some other pair is sent instead.

Definition 3.1 (Strawman Auction). *Let Commit$(\cdot,\cdot)$ be a commitment scheme satisfying Assumption 2.1. For a given direct revelation mechanism, with allocation rule $\vec{x}(\cdot)$ and payment rule $\vec{p}(\cdot)$,* Strawman$(\vec{x}, \vec{p})$ *is the following auction:*

1^{st} *Round:*

- *Each bidder i picks a bid, b_i, draws r_i uniformly at random, and sends $c_i := \text{Commit}(b_i, r_i)$.*
- *The auctioneer sends each commitment to all buyers.*

2^{nd} *Round:*

- *Each bidder i sends (b_i, r_i) to the auctioneer.*
- *The auctioneer forwards each (b_i, r_i) to all buyers.*

Resolution:

- *Let S denote the set of bidders for which $c_i = \text{Commit}(b_i, r_i)$, and let $b'_i := b_i \cdot I(i \in S)$. Allocate and charge payments according to $\vec{x}(\vec{b}'), \vec{p}(\vec{b}')$.*

[3]For a discrete distribution, the hazard rate $h(x)$ is $\Pr[v = x]/\Pr[v > x]$, and the virtual value $\varphi(x)$ is still $x - 1/h(x)$.

In particular, observe that, importantly, the auction's behavior must be well-defined even when not all commitments are revealed. We quickly observe that the Strawman Auction preserves incentive compatibility:

Observation 3.1. *Let $(\vec{x}, \vec{p})$ be a strategyproof, individually rational, direct revelation mechanism. Then* $\mathsf{Strawman}(\vec{x}, \vec{p})$ *is also strategyproof and individually rational. In particular, it is an ex-post Nash for each bidder to set $b_i := v_i$, and to reveal in round two.*

Proof. Because $(\vec{x}, \vec{p})$ is individually rational, no bidder can benefit by replacing their bid with 0 by concealing in round two. Given that bidder i will reveal, and that all other bidders will also reveal,[4] it is best for bidder i to commit to v_i (because $(\vec{x}, \vec{p})$ is strategyproof). □

Observation 3.1 establishes that this modification preserves strategyproofness. One might hope that it also encourages the auctioneer to behave honestly (if $\vec{x}, \vec{p}$ is the revenue-optimal auction) because they do not know any of the buyers' bids before round two. So while the auctioneer can create fake bidders and submit fake bids, it seems like these bids may simply act as a reserve. And indeed, *if the auctioneer must reveal all fake bids*, the only reasonable deviations are to reveal the precise fake bids selected in round one (which was chosen with no information about buyers' values). Therefore, the Strawman optimal auction would be computationally credible by the same reasoning used in [AL19] for the ascending price auction.

Unfortunately, the auction's behavior must be well-defined even when some bids are concealed, and the auction cannot merely stall. For example, bidders may naturally drop out between rounds due to latency issues, or attackers may adversarially bid and conceal to stall the system. Restarting the auction is perhaps even worse, as now the auctioneer has learned some private information from those bidders who did participate honestly. This means that while it is not a safe, reasonable deviation for the auctioneer to change their commitment, it is indeed a safe, reasonable deviation for the auctioneer to simply conceal some fake bids. The following example establishes that such deviations violate computational credibility of the Strawman auction.

Example 3.1 (Strawman is not computationally credible). *Consider that there is a single (real) buyer, whose value is drawn uniformly from $\{1, 2\}$, and consider the Strawman second-price auction with reserve 1, which tie-breaks lexicographically. The auctioneer will get expected revenue 1 by being honest (which is optimal among all strategyproof auctions). Instead, they could create a fake bidder, and always commit to $b_2 = 2$. After bidder 1 reveals in round 2, the auctioneer can either (a) reveal b_2, if $b_1 = 2$, causing $b'_2 = 2$ and yielding revenue 2 or (b) conceal, if $b_1 = 1$, causing $b'_2 = 0$ and yielding revenue 1. This gets the auctioneer expected revenue $3/2$.*

The main takeaway from this section is that the Strawman auction serves as a good base for a computationally credible, strategyproof auction; however, we cannot force the auctioneer (or any bidder, for that matter) to reveal their bids. Our solution in Section 4 is to instead fine all bidders (including fake bidders) who conceal, to disincentivize this particular safe, reasonable deviation.

4 DEFERRED REVELATION AUCTION

In this section, we describe the Deferred Revelation Auction (DRA) and prove basic facts that will be useful throughout all of our analyses. Rather than state the auction as a reduction, we directly apply it to Myerson's revenue-optimal auction. Below, recall that $\bar{\varphi}(\cdot)$ is Myerson's ironed virtual value function, which is the upper concave envelope of $\varphi(\cdot)$ (for further details, see [Mye81, Har13]).

[4] Note that this is necessary: it is not a *dominant strategy* to be honest. Bidder 1 could use a weird strategy "Commit to $c_1 := (\infty, 0)$. If I am sent a commitment of $c = \mathsf{Commit}(5, 12)$, then conceal. Otherwise, reveal." If bidder 1 uses this strategy (and you are the only other bidder), it is a better response to just send $\mathsf{Commit}(5, 12)$ and reveal, rather than being honest.

Definition 4.1 (Deferred Revelation Auction). *Let Commit$(\cdot,\cdot)$ be a commitment scheme satisfying Assumption 2.1. For a given* fine function $f(\cdot,\cdot)$, DRA(f) *is the following auction:*

1^{st} Round:

- *Each buyer i picks a bid, b_i, draws a one-time pad r_i uniformly at random, and sends $c_i :=$ Commit(b_i, r_i). The distribution D_i from which v_i is drawn is known to the auctioneer.*
- *The auctioneer sends (c_i, D_i, i) to all buyers. Let n_i denote the number of pairs sent to buyer i (including their own).*

2^{nd} Round:

- *Each buyer i sends (b_i, r_i) to the auctioneer.*
- *The auctioneer forwards each (b_i, r_i) to all buyers.*

Resolution:

- *Let S denote the set of buyers for which $c_i =$ Commit(b_i, r_i), and let $b'_i := b_i \cdot I(i \in S)$. Let $i^* :=$ arg $max_{i \in S}\{\bar{\varphi}_i(b_i)\}$.*
- *If $\bar{\varphi}_{i^*}(b_{i^*}) > 0$, award buyer i^* the item. Charge them $\bar{\varphi}_i^{-1}(max\{0, max_{i \in S\setminus\{i^*\}}\{\bar{\varphi}_i(b_i)\}\})$.*[5]
- *Additionally, all $i \notin S$ pay buyer i^* a fine equal to $f(n_{i^*}, D_{i^*})$.*

Tie-breaking:

- *All ties are broken lexicographically, with the auctioneer treated as "buyer zero". With this, we will write all inequalities as $>$ or $<$, taking this tie-breaking already into account.*

Above, we are essentially running the optimal Strawman auction, but fining any buyers who conceal *and paying these fines to the winning buyer.* Intuitively, this helps in the following way: during round one, the auctioneer can certainly gamble and commit to several fake bids. However, they run the risk of accidentally overshooting the winning bid. In the Strawman auction, they could simply conceal these bids. In DRA(f), they must instead pay some fine $f(n_{i^*}, D_{i^*})$. Intuitively, it seems that if the fine is large enough, the auctioneer would rather just be honest than commit to any fake bids and run the risk of paying a huge fine. This turns out to be true when each D_i is MHR, but not in general. Before stating our main results, we recap the safe, reasonable deviations.

(1) The seller might create fake buyers during round one.
(2) The seller may selectively choose which commitments to send to buyer i.
    - The seller might not send c_j at all.
    - The seller might send c_j, but with some D'_j instead of the true D_j.
    - If Commit$(\cdot,\cdot)$ were malleable, the seller could apply some function $g(\cdot)$ to b_j and forward instead $c'_j =$ Commit$(g(b_j), r_j)$. We assumed in Assumption 2.1 that Commit$(\cdot,\cdot)$ is non-malleable to avoid this, although Theorem 4.1 holds even without this assumption.
    - All of these might depend on $\vec{b}_{-i}$, but not b_i.[6]
(3) The seller might conceal a commitment. This decision can depend on the entire $\vec{b}$.

Before reasoning about computational credibility, we quickly observe that DRA(f) is indeed strategyproof and optimal.

Observation 4.1. *For all f,* DRA(f) *is strategyproof and revenue-optimal.*

[5] Here, we define the inverse of a monotone function $g(\cdot)$ to be $g^{-1}(y) = \inf_x\{x \mid g(x) \geq y\}$.

[6] For example, the seller might solicit a commitment from all buyers. Then, in increasing order of i, they could forward some commitments to buyer i, and ask i to reveal. Then, after terminating this for all buyers, they could go back and reveal commitments. As far as any individual buyer can tell, the timeline appears correct based on their interaction with the seller.

Proof. DRA(f) is clearly optimal, as it simply runs Myerson's auction. It is also strategyproof: because Myerson's auction is individually rational, buyers have no incentive to conceal their commitment in round two. Given that all buyers will reveal their commitments, it is in buyer i's interest to commit to v_i, because Myerson's auction is truthful. □

It is more challenging to reason when DRA(f) is computationally credible. While there are many ways the seller might deviate, our approach to upper bounding the seller's revenue, fortunately, boils down to one vector of parameters determined by the seller's decisions during round one.

Definition 4.2. *For a triple* $(c_j = Commit(b_j, r_j), D_j, j)$ *sent to bidder i, denote the* effective bid *by* $\beta_{ij} := \bar{\varphi}_i^{-1}(\bar{\varphi}_j(b_j))$. *We call the* effective commitment *to buyer i as* $\beta_i := max\{\bar{\varphi}_i^{-1}(0), max_j\{\beta_{ij}\}\}$. *We call the* effective reveal *to buyer i as* $\gamma_i := max\{\bar{\varphi}_i^{-1}(0), max_{j,c_j \text{ is revealed to } i}\{\beta_{ij}\}\}$.

Recall that β_i *is a function only of* $\vec{b}_{-i}$, *and* γ_i *is a function of* β_i *and* $\vec{b}$.

Observation 4.2. *For all f, under any safe, reasonable deviation to* DRA(f), *bidder i receives the item if and only if* $v_i > \gamma_i$. *Therefore,* $v_i > \gamma_i$ *for at most one bidder.*

We now quickly show that Observation 4.2 is enough to show that DRA(f) is computationally credible whenever each D_i is bounded.

Observation 4.3. *Let each* D_i *be bounded, and let* $f(n, D_i) := \inf\{x : \Pr_{v \leftarrow D_i}[v > x] = 0\} + 1$. *Then* DRA($f$) *is optimal, strategyproof, and computationally credible for the instance* $D = \times_i D_i$.

Proof. Optimality and strategyproofness follow directly from Observation 4.1. To see that DRA(f) is computationally credible, observe that the auctioneer will certainly get negative revenue if they ever conceal a fake bid sent to buyer i and sell them the item (because buyer i will pay at most $\inf\{x : \Pr_{v \leftarrow D_i}[v > x] = 0\}$, while the auctioneer must pay a strictly larger fine). Therefore, any optimal safe, reasonable deviation has $v_i < \gamma_i \Leftrightarrow v_i < \beta_i$. Indeed, the $\Leftarrow$ implication is trivial, as $\gamma_i \le \beta_i$. The $\Rightarrow$ implication follows because the auctioneer would get negative revenue selling the item to buyer i, and could strictly improve their revenue by just revealing all commitments and not selling the item.

Once we have this implication, observe that buyer i now wins the item if and only if $v_i > \beta_i$, and β_i is a function of $\vec{b}_{-i}$. Moreover, when buyer i wins, they will pay β_i. This is a truthful mechanism, and therefore it achieves revenue no better than Myerson's optimal auction. To recap: we have shown that every safe, reasonable deviation is strictly outperformed by another deviation, which implements a truthful mechanism, which is outperformed by executing the auction in earnest. □

Observation 4.3 illustrates one idea to reason about computational credibility of DRA(f), but does not really shed much insight, as it is essentially just forcing the auctioneer to reveal all commitments. Our main results, therefore, concern unbounded distributions (or significantly shrinking the fines necessary for bounded distributions), where there do not exist sufficiently large fines to trivially force the auctioneer to always reveal. We begin with our positive results. Below, $r(D_0)$ denotes the Myerson reserve for a one-dimensional distribution D_0.

Theorem 4.1. *Let* $f(n, D_i) := r(D_i)$.[7] *Then when all* D_i *are MHR (bounded or unbounded),* DRA(f) *is optimal, strategyproof, and computationally credible.*

Theorem 4.2. *For all* $\varepsilon, \alpha > 0$, *there exists an* $f(\cdot, \cdot)$ *such that* $f(n, D_i) \le poly_\alpha(n, r(D_i), 1/\varepsilon)$ *for all* n, D_i,[8] *such that when all* D_i *are unbounded and* α*-strongly regular,* DRA(f) *is optimal, strategyproof, and computationally* ε*-credible.*

[7]Note that when D_i is MHR, $r(D_i) = \Theta(\text{Rev}(D_i))$ [CD11].

[8]By the notation $\text{poly}_\alpha(\cdot)$, we mean that for all fixed α, the fine is $\text{poly}(n, D(r_i), 1/\varepsilon)$.

Theorem 4.2 can be improved to remove the ε when there is just a single bidder, but not otherwise (see Theorem 4.4 shortly after).

Proposition 4.1. *Moreover, for all $\alpha > 0$, there exists an $f(\cdot,\cdot)$ with $f(n, D_0) := \Theta_\alpha(r(D_0))$ for all n, such that when D_0 is α-strongly regular,* DRA(f) *is optimal, strategyproof, and computationally credible when there is a single (real) buyer from D_0.*

Theorem 4.1 is our main positive result: it asserts that there is a reasonably-sized fine, which depends only on D_i and not even on n, such that these fines are sufficient to deter the auctioneer from submitting fake bids. Proposition 4.1 extends Theorem 4.1 to α-strongly regular distributions when there is just a single (real) bidder. Theorem 4.2 is an extension to multiple bidders, but is a relaxation in two ways: the mechanism is only ε-credible, and the fine now depends on n. Our main negative results establish that these are necessary, and Theorem 4.2 is essentially the limit of what DRA(f) achieves within the framework of α-strongly regular distributions. Our negative results are as follows:

Theorem 4.3. *There exists an unbounded regular distribution D_0, such that for all $f(\cdot,\cdot)$,* DRA(f) *is* not *computationally ε-credible for the instance D_0 and* any $\varepsilon < 1$.

Theorem 4.4. *For all $f(\cdot,\cdot)$, all $\alpha < 1$, and all $n > 1$, there exists an unbounded D_0 that is α-strongly regular such that* DRA(f) *is* not *computationally credible for the instance $D := \times_{i=1}^{n} D_0$.*

Before continuing, let us parse the results, which clearly distinguish between MHR, α-strongly MHR, and regular distributions. On one extreme, DRA works as well as could be hoped for when all distributions are MHR: there is a fine which is *independent of the number of buyers* which suffices to ensure that DRA is computationally credible. On the other extreme, DRA does not work well at all for arbitrary regular distributions: even when $n = 1$, there may not exist a sufficiently large fine to discourage the auctioneer from cheating, and cheating may yield unboundedly more revenue than honesty. In the middle, we see that Theorem 4.2 does not distinguish between different values of $\alpha \in (0, 1)$. In this range, positive results are possible, but not quite so strong as for MHR distributions. Moreover, the positive results we prove are tight.

We conclude this section by revisiting our simple example under DRA instead of Strawman. Section 5 follows immediately afterwards, and proves Theorem 4.3 (perhaps unsurprisingly, the witness D_0 is the equal-revenue curve). This will give an intuition for the technical challenges, and why stronger assumptions are necessary to have the positive results in Theorems 4.1 and 4.2, whose proofs follow in Sections 6 and 7.

Example 4.1. *Consider that there is a single (real) buyer, whose value is drawn from D_1, which is the uniform distribution on $\{1, 2\}$. Let also $f(n, D_1) := 1$ for all n. Consider now the auction* DRA(f). *The auctioneer will get expected revenue 1 by being honest and not submitting any fake bids (which is optimal among all strategyproof auctions). Instead, the auctioneer could submit any number of fake bids. It is clear that it only makes sense to submit fake bids of 2, and also that it is unnecessary to submit multiple fake bids of the same value.*

In order to be a reasonable deviation, if the auctioneer submits a fake bid of $b_2 = 2$, then after buyer 1 reveals in round 2, the auctioneer can either reveal $b_2 = 2$, or conceal. In order to be a safe deviation, the auctioneer must set a price of b_2 to buyer 1 if they reveal, and set a price of 1 otherwise. In particular, observe that while the auctioneer can guarantee revenue 2 when $b_1 = 2$ (by revealing), the best revenue they can guarantee when $b_1 = 1$ is 0. If they reveal, then they pay no fines but also receive no payment. If they conceal, then they get payment of 1, but also pay a fine of 1, for a net payment of 0. Therefore, no matter what strategy the auctioneer uses, they get revenue at most 1 in expectation, the same as being honest.

Observe that if we only consider safe *(but unreasonable) deviations, then the auctioneer could commit to $b_2 = 2$, but reveal instead a commitment to $b_2 = 1$ when $b_1 = 1$. Of course, doing so would require breaking the cryptographic commitment scheme, an event that can be made less likely than the inverse number of atoms in the universe. So this mechanism is not* credible*, but only* computationally credible*, and this example highlights the distinction.*

5 EXAMPLE: DRA ON REGULAR DISTRIBUTIONS

In this section, we prove Theorem 4.3. The main intuition is that the equal-revenue curve is so heavy-tailed that no matter how big the fines are, there are always some sufficiently-high fake bids that the auctioneer can set to extract additional revenue while barely ever paying the fine.

Proof of Theorem 4.3. Let D_0 denote the equal-revenue distribution, which has CDF $1 - 1/x$ on $[1, \infty)$. The optimal revenue that the seller can achieve by earnestly running a truthful auction for one bidder drawn from D_0 is 1. Consider now any fine function $f(\cdot, \cdot)$, and simply refer to $L_n := f(n + 1, D_0)$ as the fine the seller must pay per hidden fake bid, if they submit n fake bids. We show in fact that for all $f(\cdot, \cdot)$, there not only exists a safe, reasonable deviation which achieves revenue > 1, but also one that achieves revenue $> r$ *for any* r.

For a given r, let $n \geq r+2$. Consider now the following construction of fake bids: Set $b_i := n^{2i} \cdot L_n$ for all $i \in [n]$. For simplicity of notation, define $b_{n+1} := \infty$. The seller's strategy is then:

- Commit to a bid b_i for all $i \in [n]$.
- When the bidder's bid, b, is revealed:
  - If $b < b_1$, reveal all bids.
  - Otherwise, if $b \in [b_i, b_{i+1})$, reveal bids $b_1, \ldots, b_i$, and conceal $b_{i+1}, \ldots, b_n$.

We now want to compute the seller's expected revenue for this strategy. We do this by first upper bounding the total expected *fines* that the seller will pay.

Claim 5.1. *The total expected fines paid by the seller in expectation is at most* $1/n$.

Proof. Observe that the seller only ever pays a fine when $b > b_1$. Because b is drawn from the equal-revenue curve, this occurs with probability at most $1/b_1 = 1/(n^2 L_n)$. Moreover, the seller submits only n fake bids, and therefore the total fine they pay, conditioned on paying a fine at all, is at most nL_n. Therefore, the total expected fines paid by the seller in expectation is at most $1/n$. □

Next, we show that the seller's expected payment received by the buyer is still large.

Claim 5.2. *The expected revenue that the seller receives is at least* $n - 1/n$.

Proof. We compute the probability that the buyer pays exactly b_i, for all i. Observe that the buyer pays exactly b_i whenever $b \in [b_i, b_{i+1}]$ which occurs with probability exactly $1/b_i - 1/b_{i+1}$, because b is drawn from the equal-revenue curve. As $b_{i+1} = n^2 b_i$, this probability is exactly $(1 - 1/n^2)/b_i$ (or this is a lower bound, when $i = n$). Therefore, the expected revenue can be written as:

$$\sum_{i=1}^{n} b_i \cdot \Pr[\text{buyer pays exactly } b_i] \geq b_i \cdot (1 - 1/n^2)/b_i = n - 1/n.$$

□

Claims 5.1 and 5.2 together establish that the seller achieves expected revenue at least $n - 2/n \geq r$, as desired. □

The key feature of the equal-revenue curve which drives the proof of Theorem 4.3 is that for all probabilities p, there exists an optimal reserve which is exceeded with probability at most

p. This allowed us to set extremely high "reserves", to get revenue as if we are setting each of these reserves independently, while also paying fines so extremely rarely that it barely matters. In Appendix D, we show that it is really a condition like this which drives Theorem 4.3, and not just that the equal-revenue curve has infinite expectation (by providing an example of a distribution with infinite expectation and a choice of f for which DRA(f) is computationally ε-credible for that distribution). We will also try to use this as intuition when explaining our (more technical) proofs for the MHR and α-strongly regular cases.

6 DRA IS CREDIBLE FOR MHR DISTRIBUTIONS

In this section, we consider the performance of DRA on MHR distributions. Drawing intuition from what drove the proof of Theorem 4.3, the key feature which enables a strong positive result for (even unbounded) MHR distributions is that the revenue generated by reserves significantly above the optimum shrinks exponentially fast.

Recall from Section 4 that β_i denotes the effective commitment to buyer i, and that it is a function of $\vec{b}_{-i}$. Our analysis breaks down the expected revenue achieved by the seller using any round one strategy into two terms: revenue from cases where there exists an i such that $b_i > \beta_i$, and revenue when all i satisfy $b_i < \beta_i$. The first case, which we proceed with now, has similarities to the analysis in Section 4, but is more precise so that it can be combined with the second case.

Lemma 6.1. *For any D, f, consider any strategy of the seller, which is a safe, reasonable deviation to* DRA(f). *Let $R(\vec{b})$ denote the revenue achieved by the seller on bids $\vec{b}$ using this strategy. Then:*

$$\mathbb{E}_{\vec{v} \leftarrow D}[R(\vec{v}) \cdot I(\exists\, i, v_i > \beta_i)] \leq \mathbb{E}_{\vec{v} \leftarrow D}[max_j\{\varphi_j(v_j)\} \cdot I(\exists\, i, v_i > \beta_i)].$$

Proof. Observe first that by Observation 4.2, whenever there exists an i such that $v_i > \beta_i$, there is a unique such i (otherwise, each such i certainly satisfies $v_i > \gamma_i$ as $\gamma_i \leq \beta_i$, which contradicts Observation 4.2). So consider the allocation rule which awards the item to bidder i if and only if $v_i > \beta_i$, and charges them β_i. Observe first that the expected revenue of this allocation rule is *at least* $\mathbb{E}_{\vec{v} \leftarrow D}[R(\vec{v}) \cdot I(\exists\, i, v_i > \beta_i)]$. Indeed, if the seller chooses to reveal all commitments sent to bidder i, then this will be exactly the expected revenue. If the seller (suboptimally) chooses instead to conceal some, they simply pay additional fines and get less revenue.

Importantly, observe also that this allocation rule is monotone, as β_i doesn't depend on v_i. Moreover, observe that this allocation/payment rule is truthful. Therefore, Myerson's Lemma implies that its expected revenue is exactly its expected virtual surplus, and its expected virtual surplus is exactly $\mathbb{E}_{\vec{v} \leftarrow D}[\sum_i \varphi_i(v_i) \cdot I(v_i > \beta_i)]$. This gives the following chain of inequalities:

$$\begin{aligned}
\mathbb{E}_{\vec{v} \leftarrow D}\left[R(\vec{v}) \cdot I(\exists\, i, v_i > \beta_i)\right] &\leq \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_i \beta_i \cdot I(v_i > \beta_i)\right] \\
&= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_i \varphi_i(v_i) \cdot I(v_i > \beta_i)\right] \\
&\leq \mathbb{E}_{\vec{v} \leftarrow D}\left[\max_j\{\varphi_j(v_j)\} \cdot I(\exists\, i, v_i > \beta_i)\right].
\end{aligned}$$

The first line follows from the reasoning in the first paragraph: DRA(f) will charge bidder i at most β_i when they win. The second line is just Myerson's lemma. The final line is just upper bounding a particular virtual value with the maximum virtual value and uses Observation 4.2 to conclude that no more than one indicator variable in the sum can be non-zero. □

The second step is now to bound the optimal revenue the seller can get from cases where $v_i < \beta_i$ for all i. The following technical lemma will be a crucial step in this part of the analysis. Intuitively, Lemma 6.2 states that the expected *value* of a draw from an MHR distribution, conditioned on being large, is not much more than its expected *virtual value* under the same conditioning. Below, recall that we defined $r(D_0)$ to be the Myerson reserve of D_0.

LEMMA 6.2. *Let D_0 be MHR. Let E be any event such that $\Pr_{v \leftarrow D_0}[v \geq r(D_0)|E] = 1$. Then:*

$$\mathbb{E}_{v \leftarrow D_0}[v|E] \leq \mathbb{E}_{v \leftarrow D_0}[\varphi(v)|E] + r(D_0).$$

Equivalently, $\mathbb{E}_{v \leftarrow D_0}[v \cdot I(E)] \leq \mathbb{E}_{v \leftarrow D_0}[\varphi(v) \cdot I(E)] + r(D_0) \cdot \Pr[E]$.

PROOF. Recall that because D_0 is MHR, and $v \geq r(D_0)$, we have that $\varphi(v) - \varphi(r(D_0)) \geq v - r(D_0)$ whenever event E occurs. Recalling that $\varphi(r(D_0)) = 0$ by definition, this rearranges to $v \leq r(D_0) + \varphi(v)$. We then immediately conclude:

$$\begin{aligned}
\mathbb{E}_{v \leftarrow D_0}[v|E] &\leq \mathbb{E}_{v \leftarrow D_0}[\varphi(v) + r(D_0)|E] \\
&= \mathbb{E}_{v \leftarrow D_0}[\varphi(v)|E] + r(D_0).
\end{aligned}$$

□

COROLLARY 6.1. *Let each D_i be MHR, and consider* DRA(f) *where $f(n, D_i) = r(D_i)$ for all i. Consider any strategy of the seller, which is a safe, reasonable deviation, and let $R(\vec{b})$ denote the revenue achieved by the seller on bids $\vec{b}$ using this strategy. Then:*

$$\mathbb{E}_{\vec{v} \leftarrow D}[R(\vec{v}) \cdot I(\forall\, i, v_i < \beta_i)] \leq \mathbb{E}_{\vec{v} \leftarrow D}[max\{0, max_j\{\varphi_j(v_j)\}\} \cdot I(\forall\, i, v_i < \beta_i)].$$

PROOF. For ease of notation let $r_i := r(D_i)$, and let $X_i(\vec{v})$ denote the indicator random variable for the event that $v_i > r_i$, $v_j < \beta_j$ for all j, and the item is awarded to bidder i. Then clearly when this occurs, the payment made by bidder i is at most v_i. But additionally, selling the item to buyer i when $v_i < \beta_i$ requires concealing at least one commitment and paying a fine (otherwise, bidder i expects not to win the item). As the fine charged per concealed commitment is r_i, this means that the seller's total revenue is at most $v_i - r_i$. In particular, this also concludes that the seller's total revenue when awarding the item to buyer i when $v_i < r_i$ is non-positive. Therefore, we can write:

$$\mathbb{E}_{\vec{v} \leftarrow D}[R(\vec{v}) \cdot I(\forall\, i, v_i < \beta_i)] \leq \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_i (v_i - r_i) \cdot X_i(\vec{v})\right].$$

But now let's consider $\mathbb{E}_{\vec{v} \leftarrow D}[(v_i - r_i) \cdot X_i(\vec{v})]$ separately for each i. The event $X_i(\vec{v}) = 1$ satisfies the hypotheses of Lemma 6.2, as $X_i(\vec{v}) = 1$ implies that $v_i > r_i$. Therefore, Lemma 6.2 allows us to conclude that:

$$\begin{aligned}
\mathbb{E}_{\vec{v} \leftarrow D}[(v_i - r_i) \cdot X_i(\vec{v})] &= \mathbb{E}_{\vec{v} \leftarrow D}\left[v_i \cdot X_i(\vec{v})\right] - r_i \cdot \Pr[X_i(\vec{v}) = 1] \\
&\leq \mathbb{E}_{\vec{v} \leftarrow D}\left[\varphi_i(v_i) \cdot X_i(\vec{v})\right].
\end{aligned}$$

The first line is just linearity of expectation, and the second line follows by Lemma 6.2. Now, we can put everything together to conclude:

$$
\begin{aligned}
\mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v})\cdot I(\forall\, i, v_i < \beta_i)] &\le \mathbb{E}_{\vec{v}\leftarrow D}\left[\sum_i \varphi_i(v_i)\cdot X_i(\vec{v})\right] \\
&\le \mathbb{E}_{\vec{v}\leftarrow D}\left[\max_i\{\varphi_i(v_i)\}\cdot\left(\sum_i X_i(\vec{v})\right)\right] \\
&\le \mathbb{E}_{\vec{v}\leftarrow D}\left[\max\{0,\max_j\{\varphi_j(v_j)\}\}\cdot I(\forall\, i, v_i < \beta_i)\right].
\end{aligned}
$$

The first line is simply restating the work above. The second line is just upper bounding each $\varphi_i(v_i)$ with the maximum virtual value. The final line simply observes that at most one of the indicators $X_i(\vec{v})$ can be one (because at most one bidder can receive the item), and that a prerequisite for any of them to be one is that all $v_i < \beta_i$. □

Lemma 6.1 and Corollary 6.1 together suffice to prove Theorem 4.1.

Proof of Theorem 4.1. Lemma 6.1 upper bounds the expected revenue of any safe, reasonable deviation when some $v_i > \beta_i$. Corollary 6.1 upper bounds the expected revenue of any safe, reasonable deviation when all $v_i < \beta_i$. Together, this implies that for any safe, reasonable deviation:

$$
\begin{aligned}
\mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v})] &= \mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v})\cdot I(\exists\, i, v_i > \beta_i)] + \mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v})\cdot I(\forall\, i, v_i < \beta_i)] \\
&\le \mathbb{E}_{\vec{v}\leftarrow D}[\max_j\{\varphi_j(v_j)\}\cdot I(\exists\, i, v_i > \beta_i)] \\
&\quad + \mathbb{E}_{\vec{v}\leftarrow D}[\max\{0,\max_j\{\varphi_j(v_j)\}\}\cdot I(\forall\, i, v_i < \beta_i)] \\
&= \mathbb{E}_{\vec{v}\leftarrow D}[\max\{0,\max_j\{\varphi_j(v_j)\}\}].
\end{aligned}
$$

The RHS is now precisely the expected revenue that the seller achieves by executing the protocol in earnest, so this series of inequalities explicitly witnesses that every safe, reasonable deviation yields expected revenue at most that of being honest. □

To repeat the key steps in the proof: Lemma 6.1 doesn't use at all the particular form of $f(\cdot,\cdot)$, nor that each D_i is MHR. It merely says that the revenue achieved from cases where the seller may as well reveal all commitments is the same as a truthful auction (because these commitments to i are a function only of $\vec{b}_{-i}$). Corollary 6.1 uses the particular form of $f(\cdot,\cdot)$ and that each D_i is MHR to conclude that even when the seller might strategically conceal some commitments, it does no better than a truthful auction.

7 EXTENSIONS AND LIMITATIONS OF α-STRONGLY REGULAR DISTRIBUTIONS

We now provide an extension of Theorem 4.1 to α-strongly regular distributions, but also prove the limits of such an extension. The proof of our extension follows a similar outline to Section 6. In particular, recall that Lemma 6.1 held *for all distributions*, not just MHR. So we will use Lemma 6.1 verbatim to handle the case where some $v_i > \beta_i$. Lemma 6.2, however, requires the MHR assumption. Our first step is to extend (and relax) Lemma 6.2. The proof of Lemma 7.1 and Corollary 7.1 are similar to Section 6, and deferred to Appendix B.

Lemma 7.1. *Let D_0 be α-strongly regular. Let E be such that* $\Pr_{v\leftarrow D_0}[v \ge r(D_0)|E] = 1$. *Then:*

$$\mathbb{E}_{v\leftarrow D_0}[v|E] \le \frac{1}{\alpha}\cdot\mathbb{E}_{v\leftarrow D_0}[\varphi(v)|E] + r(D_0).$$

Equivalently, $\mathbb{E}_{v\leftarrow D_0}[v\cdot I(E)] \le \frac{1}{\alpha}\cdot\mathbb{E}_{v\leftarrow D_0}[\varphi(v)\cdot I(E)] + r(D_0)\cdot\Pr[E]$.

In Corollary 7.1 below, we will consider again safe, reasonable deviations from a particular DRA(f). Below, we'll let $R(\vec{b})$ denote the revenue achieved by the seller (using this particular deviation) on bids $\vec{b}$, and $k_i := f(n_i, D_i)$.

Corollary 7.1. *Let each D_i be α-strongly regular, and consider* DRA(f) *where $f(n, D_i) \geq r(D_i)$ for all n, i. Consider any strategy of the seller which is a safe, reasonable deviation. Finally, let $X_i(\vec{v})$ denote the indicator random variable for the event that the item is awarded to bidder i, $v_i > k_i$, and $v_j < \beta_j$ for all j. Then:*

$$\mathbb{E}_{\vec{v}\leftarrow D}\left[R(\vec{v}) \cdot I(\forall\, i, v_i < \beta_i)\right] \leq \sum_i \mathbb{E}_{\vec{v}\leftarrow D}\left[(\varphi_i(v_i)/\alpha + r_i - k_i) \cdot X_i(\vec{v})\right].$$

From here, making use of Corollary 7.1 is not as straight-forward as in the MHR case. We first need another technical lemma, bounding the achievable revenue by posting a very high price for a single α-strongly regular distribution. The proof of Lemma 7.2 appears in Appendix B.

Lemma 7.2. *Let D_0 be α-strongly regular. Then for all $p \geq r(D_0)$,*

$$p \cdot \Pr_{v\leftarrow D_0}[v \geq p] \leq r(D_0) \cdot \Pr_{v\leftarrow D_0}[v \geq r(D_0)] \cdot (1-\alpha)^{-1/(1-\alpha)} \cdot \left(\frac{p}{r}\right)^{-\frac{\alpha}{1-\alpha}}$$

And finally, we need one more technical lemma before we can wrap up the proof of Theorem 4.2. This technical lemma is the only reason why Theorem 4.2 applies to unbounded distributions. The proof is included, as it has no counterpart in Section 6.

Lemma 7.3. *Let each D_i be unbounded. Then for all f, all $j \in [n]$, and any safe, reasonable deviation in* DRA(f) *it must be that for at least j distinct bidders, $n_i \geq n - j + 1$. In particular, $\sum_i 1/n_i^2 \leq \pi^2/6 \leq 2$.*

Proof. For simplicity of notation, relabel the bidders $1, \ldots, n$ by the order in which the seller requests their decommitment (if some are requested simultaneously, break those ties arbitrarily). Importantly, observe that the seller cannot request decommitment from a bidder until they have forwarded all commitments. Therefore, the decision of which commitments to forward to bidder i can depend only on $\vec{b}_{<i}$.

So now assume for contradiction that the lemma fails for some j. Then there is some bidder $i \leq j$ with $n_i \leq n - i$ (recall that n_i includes their own commitment too). In particular, this means that there is some bidder $\ell > i$ whose commitment was not forwarded to bidder i, and that b_ℓ was completely unknown when this decision was made. In particular, the following situation now has non-zero probability:

- First, draw $v_{-i,\ell}$ to determine which commitments to forward to bidder i. Observe that this also suffices to define β_i, as it is independent of both v_i and v_ℓ.
- Now, it is entirely possible that $v_i > \beta_i$, as D_i is unbounded. Observe that determining this only requires additionally drawing v_i.
- Now, this sets β_ℓ. As we have yet to draw v_ℓ, it is entirely possible that $v_\ell > \beta_\ell$, as D_ℓ is unbounded.

The above derives a contradiction to the deviation being safe and reasonable, as now two distinct buyers are both expecting to win the item. The "In particular,…" part of the statement follows simply as the sum is minimized when there is exactly one bidder with $n_i = j$, for all $j \in [n]$. □

We can now wrap up the proof of Theorem 4.2.

Proof of Theorem 4.2. Consider first combining Lemma 6.1 and Corollary 7.1. If we set $f(n, D_i) := \left(\frac{2n^2}{\varepsilon\alpha}\right)^{\frac{1-\alpha}{\alpha}} \cdot (1-\alpha)^{-1/\alpha} \cdot r(D_i)$, we get:

$$\begin{aligned}
\mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v})] &= \mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v}) \cdot I(\exists\, i, v_i > \beta_i)] + \mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v}) \cdot I(\forall\, i, v_i < \beta_i)] \\
&\leq \mathbb{E}_{\vec{v}\leftarrow D}[\max_j\{\varphi_j(v_j)\} \cdot I(\exists\, i, v_i > \beta_i)] + \sum_i \mathbb{E}_{\vec{v}\leftarrow D}\left[(\varphi_i(v_i)/\alpha + r(D_i) - k_i) \cdot X_i(\vec{v})\right] \\
&\leq \mathbb{E}_{\vec{v}\leftarrow D}[\max\{0, \max_j\{\varphi_j(v_j)\}\}] + \sum_i \mathbb{E}_{v_i\leftarrow D_i}\left[\varphi_i(v_i) \cdot (1/\alpha) \cdot I(v_i > k_i)\right] \\
&= \mathbb{E}_{\vec{v}\leftarrow D}[\max\{0, \max_j\{\varphi_j(v_j)\}\}] + \sum_i k_i \cdot \Pr_{v_i\leftarrow D_i}[v_i > k_i]/\alpha \\
&\leq \mathbb{E}_{\vec{v}\leftarrow D}[\max\{0, \max_j\{\varphi_j(v_j)\}\}] \\
&\qquad + \sum_i (1-\alpha)^{-1/(1-\alpha)} \cdot (k_i/r(D_i))^{-\frac{\alpha}{1-\alpha}} \cdot r(D_i) \cdot \Pr_{v_i\leftarrow D_i}[v_i \geq r(D_i)]/\alpha \\
&\leq \mathbb{E}_{\vec{v}\leftarrow D}[\max\{0, \max_j\{\varphi_j(v_j)\}\}] + \sum_i \frac{\varepsilon}{2n_i^2} \cdot r(D_i) \cdot \Pr_{v_i\leftarrow D_i}[v_i \geq r(D_i)] \\
&\leq \mathsf{Rev}(D) + \varepsilon \mathsf{Rev}(D) \cdot \sum_i \frac{1}{2n_i^2} \\
&\leq (1+\varepsilon)\mathsf{Rev}(D).
\end{aligned}$$

The first line is just linearity of expectation. The second line is Lemma 6.1 and Corollary 7.1. The third line simply observes that $X_i(\vec{v}) = 1 \Rightarrow v_i > k_i$, and also that $k_i > r(D_i)$. The fourth simply observes that the right-hand term of line three is the expected virtual welfare of an auction (which sells the item to bidder i whenever $v_i > k_i$), and the right-hand term of line four is the expected revenue of that same auction (so they are equal by Myerson's lemma). The fifth is a direct application of Lemma 7.2. The sixth uses our particular choice of $f(n, D_i)$. The seventh simply observes that both $\mathbb{E}_{\vec{v}\leftarrow D}[\max\{0, \max_j\{\varphi_j(v_j)\}\}] = \mathsf{Rev}(D)$, and also $r(D_i) \cdot \Pr_{v_i\leftarrow D_i}[v_i \geq r(D_i)] \leq \mathsf{Rev}(D)$ (because this is just the revenue of selling only to bidder i). The final line follows directly from Lemma 7.3. □

It may seem odd that Theorem 4.2 requires both that the distributions are unbounded, and also that the commitment scheme is non-malleable (given that neither assumption is necessary for Theorem 4.1). Both of these assumptions show up only in the proof of Lemma 7.3, where we show that the auctioneer must send many commitments to each bidder. This perhaps seems like a technical artifact of the current proof approach, but surprisingly we show that both assumptions are necessary. Specifically, Theorem 4.2 *does not* hold when the commitment scheme is malleable, nor when the distributions are bounded. This establishes that there is (perhaps surprisingly) something integral about Lemma 7.3 to the proof of Theorem 4.2. See Appendix E for formal theorem statements and proofs.

A full proof of Proposition 4.1 appears in Appendix C, which reuses several technical lemmas.

7.1 Limits of DRA for α-Strongly Regular

We conclude by establishing that the ε in Theorem 4.2 cannot be improved for $n > 1$ bidders (whereas Proposition 4.1 removes it for $n = 1$ bidder). We provide a complete proof below, which will give further intuition for why the ε is not needed for MHR distributions, or only a single bidder.

Proof of Theorem 4.4. For any $n > 1$, our safe, reasonable strategy will do the following. First, it will always interact honestly with bidders $\neq 1$. Also, it will *almost always* also interact honestly with bidder 1. In the extremely rare case that the maximum bid from bidders $\neq 1$ is unusually high, then it will try to cheat bidder 1. To be clear, the auctioneer's strategy will do the following (for simplicity of notation in what follows, we denote by $k := f(n+1, D_0)$). :

(1) Honestly solicit commitments from all n bidders.
(2) Honestly forward all commitments to all bidders $\neq 1$, and ask for them to reveal. Let $j^* := \arg\max_{j\neq 1}\{b_j\}$.
(3) If $b_{j^*} \leq T$, for some threshold T to be set later, honestly forward all commitments to bidder 1 as well, and ask bidder 1 to reveal. Execute the auction honestly.
(4) If instead $b_{j^*} > T$, forward instead all commitments to bidder 1, along with one fake commitment to $b = b_{j^*} + k$.
   - If $v_1 \leq T$, reveal b and execute the auction honestly.
   - If $v_1 \geq b$, reveal b and execute the auction honestly.
   - If $v_1 \in (T, b)$, conceal b and sell the item to bidder one.

Observe that this is indeed a safe, reasonable deviation. From the perspective of each bidder, they first send a commitment, then receive commitments, then reveal their commitment, then learn which commitments are revealed/concealed. Intuitively, our proof will show that no matter how large $f(n+1, D_0)$ is, there is always a sufficiently large T such that this fine becomes negligible and the increased revenue from setting a slightly higher "reserve" of b becomes worth it (note, however, that this phenomenon does *not* occur for MHR distributions, by Theorem 4.1).

Our distribution D_0 will have the following CDF and PDF:

$$F^\alpha(v) = \begin{cases} 0 & , v < 1 \\ 1 - \left(\frac{1}{v}\right)^{\frac{1}{1-\alpha}} & , v \geq 1 \end{cases} \qquad f^\alpha(v) = \begin{cases} 0 & , v < 1 \\ \frac{1}{1-\alpha}\left(\frac{1}{v}\right)^{\frac{2-\alpha}{1-\alpha}} & , v \geq 1 \end{cases}$$

The hazard rate of F^α is $h^{F^\alpha}(v) = \frac{1}{(1-\alpha)v}$ for $v \geq 1$ and the virtual value function of F^α is $\varphi^{F^\alpha}(v) = v - \frac{1}{h^{F^\alpha}(v)} = \alpha v$, so D_0 is α-strongly regular.

Observe that for our particular deviation, the revenue of the honest execution and our deviation differ *only when* $v_1 > v_{j^*} > T$. The tradeoff the auctioneer chooses is that when $v_1 > v_{j^*} + k$, they get an additional revenue of k. But if instead $v_1 \in (v_{j^*}, v_{j^*} + k)$, they have to pay a fine of k. Observe that the difference in both cases is exactly k, one in favor of cheating, and the other in favor of being honest. So we just want to check how big v_{j^*} needs to be in order to have $\Pr[v_1 > v_{j^*} + k] > \Pr[v_1 \in (v_{j^*}, v_{j^*} + k)]$. Again, observe that Theorem 4.1 establishes that no such v_{j^*} exists when D_0 is MHR and $k = r(D_0)$. But slightly relaxing this condition to α-strongly regular for $\alpha < 1$ now implies the existence of such a v_{j^*} for any k.

We upper bound the probability that $v_1 \in (v_{j^*}, v_{j^*} + k)$, conditioned on $v_1 \geq v_{j^*}$ (holds for any $v_{j^*} \geq 1$):

$$\begin{aligned} \Pr[v_1 \in (v_{j^*}, v_{j^*} + k) | v_1 \geq v_{j^*}] &= \int_{v_{j^*}}^{v_{j^*}+k} \frac{f^\alpha(v)}{1 - F^\alpha(v_{j^*})} dv \\ &\leq \int_{v_{j^*}}^{v_{j^*}+k} \frac{f^\alpha(v_{j^*})}{1 - F^\alpha(v_{j^*})} dv \\ &= k \cdot h^{F^\alpha}(v_{j^*}) = \frac{k}{(1-\alpha)v_{j^*}} \end{aligned}$$

Observe this also implies $\Pr[v_1 \geq v_{j^*} + k | v_1 \geq v_{j^*}] = 1 - \Pr[v_1 \in (v_{j^*}, v_{j^*} + k) | v_1 \geq v_{j^*}] \geq 1 - \frac{k}{(1-\alpha)v_{j^*}}$. Together, these two claims immediately imply that (after multiplying both by $\Pr[v_1 \geq v_{j^*}]$):

$$v_{j^*} > \frac{2k}{1-\alpha} \Rightarrow \Pr[v_1 \geq v_{j^*} + k] > \Pr[v_1 \in (v_{j^*}, v_{j^*} + k)].$$

By the work above, this proves that this deviation is strictly profitable for any $T > \frac{2k}{1-\alpha}$. □

REFERENCES

[AL19] Mohammad Akbarpour and Shengwu Li. Credible mechanisms. *Available at SSRN 3033208*, 2019.

[BK14] Iddo Bentov and Ranjit Kumaresan. How to use bitcoin to design fair protocols. In *Annual Cryptology Conference*, pages 421–439. Springer, 2014.

[BPRP08] Phillip G Bradford, Sunju Park, Michael H Rothkopf, and Heejin Park. Protocol completion incentive problems in cryptographic vickrey auctions. *Electronic Commerce Research*, 8(1-2):57–77, 2008.

[CD11] Yang Cai and Constantinos Daskalakis. Extreme-value theorems for optimal multidimensional pricing. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 522–531. IEEE, 2011.

[CDW19] Yang Cai, Nikhil R Devanur, and S Matthew Weinberg. A duality-based unified approach to bayesian mechanism design. *SIAM Journal on Computing*, (0):STOC16–160, 2019.

[Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 364–369. ACM, 1986.

[CR14] Richard Cole and Tim Roughgarden. The sample complexity of revenue maximization. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 243–252. ACM, 2014.

[DDN03] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM review*, 45(4):727–784, 2003.

[DPS14] Nikhil R Devanur, Yuval Peres, and Balasubramanian Sivan. Perfect bayesian equilibria in repeated sales. In *Proceedings of the twenty-sixth annual ACM-SIAM symposium on Discrete algorithms*, pages 983–1002. SIAM, 2014.

[FF00] Marc Fischlin and Roger Fischlin. Efficient non-malleable commitment schemes. In *Annual International Cryptology Conference*, pages 413–431. Springer, 2000.

[Gol09] Oded Goldreich. *Foundations of cryptography: volume 2, basic applications.* Cambridge university press, 2009.

[Har13] Jason D Hartline. Mechanism design and approximation. *Book draft. October*, 122, 2013.

[Hoo06] MH Hooshmand. Ultra power and ultra exponential functions. *Integral Transforms and Special Functions*, 17(8):549–558, 2006.

[ILPT17] Nicole Immorlica, Brendan Lucier, Emmanouil Pountourakis, and Samuel Taggart. Repeated sales with multiple strategic buyers. In *Proceedings of the 2017 ACM Conference on Economics and Computation*, pages 167–168, 2017.

[Kle02] Paul Klemperer. What really matters in auction design. *Journal of economic perspectives*, 16(1):169–189, 2002.

[LMSZ19] Qingmin Liu, Konrad Mierendorff, Xianwen Shi, and Weijie Zhong. Auctions with limited commitment. *American Economic Review*, 109(3):876–910, 2019.

[Mye81] Roger B Myerson. Optimal auction design. *Mathematics of operations research*, 6(1):58–73, 1981.

[NS93] Hannu Nurmi and Arto Salomaa. Cryptographic protocols for vickrey auctions. *Group Decision and Negotiation*, 2(4):363–373, 1993.

[Slu19] Sarah Sluis. Google switches to first-price auction, Mar 2019.

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations. In *FOCS*, volume 82, pages 160–164, 1982.

A FACTS ABOUT α-STRONGLY REGULAR DISTRIBUTIONS

Here we provide a proof of the main technical lemma for α-strongly regular distributions, which itself follows from two short structural lemmas. Lemma A.1 follows directly from the definition of virtual values and α-strongly regular distributions [CR14].

Lemma A.1. *If an α-strongly regular distribution has CDF F and PDF f, then for all $v' \geq v$,*

$$h(v') \geq \frac{1}{(1-\alpha)(v'-v) + 1/h(v)} \tag{1}$$

Proof. For all $v' \geq v$, if $h(v)$ is the hazard rate of F, then $\varphi(v') = 1 - 1/h(v)$. By definition of α-strongly regularity,

$$\begin{aligned} \varphi(v') - \varphi(v) = v' - 1/h(v') - v + 1/h(v) \geq \alpha(v'-v) \\ \implies 1/h(v') \leq (1-\alpha)(v'-v) + 1/h(v) \end{aligned}$$

The latter implies the statement. □

Lemma A.2. *Let an α-strongly regular distribution have CDF F and PDF f, and let $r := \varphi^{-1}(0)$. Then for all $x \geq r$,*

$$Pr_{v \leftarrow D}[v \geq x] \leq Pr_{v \leftarrow D}[v \geq r] \cdot \left(\frac{r}{(1-\alpha)x + \alpha r}\right)^{\frac{1}{1-\alpha}}$$

Proof. Let $H(v) = \int_0^v h(x)dx$. A well-known property of hazard rates is that $1 - F(v) = e^{-H(v)}$. To see this, observe that $\frac{d}{dx}\ln(1 - F(x)) = -\frac{f(x)}{1-F(x)} = -h(x)$. By the fundamental theorem of calculus, $\int_0^v -h(x)dx = \ln(1 - F(v)) - \ln(1 - F(0)) = \ln(1 - F(v))$, which implies $1 - F(v) = e^{-\int_0^v h(x)dx} = e^{-H(v)}$.

By Lemma A.1, we have

$$\begin{aligned}
H(v) = \int_0^v h(x)dx &= \int_0^r h(x)dx + \int_r^v h(x)dx \\
&\geq H(r) + \int_r^v \frac{1}{(1-\alpha)(x-r)+r}dx \\
&= H(r) + \frac{1}{1-\alpha}\Big[\ln((1-\alpha)(x-r)+r)\Big]_r^v \\
&= H(r) + \frac{1}{1-\alpha}\ln\left(\frac{(1-\alpha)v+\alpha r}{r}\right)
\end{aligned}$$

This implies that:

$$\begin{aligned}
Pr_{v \leftarrow D}[v \geq x] &= e^{-H(x)} \\
&\leq e^{-H(r)} e^{\frac{1}{1-\alpha}\ln\frac{r}{\alpha r + (1-\alpha)x}} \\
&= Pr_{v \leftarrow D}[v \geq r] \cdot \left(\frac{r}{\alpha r + (1-\alpha)x}\right)^{\frac{1}{1-\alpha}}
\end{aligned}$$

□

B OMITTED PROOFS FROM SECTION 7

Proof of Lemma 7.1. Again recall that because D_0 is α-strongly regular, and $v \geq r(D_0)$ whenever event E occurs, we have that $\varphi(v) - \varphi(r(D_0)) \geq \alpha v - \alpha r(D_0)$ whenever event E occurs. Recalling that $\varphi(r(D_0)) = 0$ by definition, this rearranges to $v \leq r(D_0) + \varphi(v)/\alpha$. We then immediately conclude:

$$\begin{aligned}
\mathbb{E}_{v \leftarrow D_0}[v|E] &\leq \mathbb{E}_{v \leftarrow D_0}[\varphi(v)/\alpha + r(D_0)|E] \\
&= \frac{1}{\alpha} \cdot \mathbb{E}_{v \leftarrow D_0}[\varphi(v)|E] + r(D_0).
\end{aligned}$$

□

Proof of Corollary 7.1. Observe first that whenever the variable $X_i(\vec{v}) = 1$, the item is awarded to bidder i, and therefore the payment made is at most v_i. But additionally, in order to sell the item to buyer i when $v_i < \beta_i$ requires concealing at least one commitment and paying a fine (otherwise, bidder i expects not to win the item). As the fine charged per concealed commitment is k_i, this means that the seller's total revenue is at most $v_i - k_i$. In particular, this also concludes that the seller's total revenue when awarding the item to buyer i when $v_i < k_i$ is non-positive. Therefore, we can write:

$$\mathbb{E}_{\vec{v}\leftarrow D}\left[R(\vec{v})\cdot I(\forall\, i, v_i < \beta_i)\right] \le \mathbb{E}_{\vec{v}\leftarrow D}\left[\sum_i (v_i - k_i)\cdot X_i(\vec{v})\right].$$

But now let's consider $\mathbb{E}_{\vec{v}\leftarrow D}\left[(v_i - k_i)\cdot X_i(\vec{v})\right]$ separately for each i. The event $X_i(\vec{v}) = 1$ satisfies the hypotheses of Lemma 7.1, as $X_i(\vec{v}) = 1$ implies that $v_i > k_i \ge r(D_i)$. Therefore, Lemma 7.1 allows us to conclude that:

$$\mathbb{E}_{\vec{v}\leftarrow D}\left[(v_i - k_i)\cdot X_i(\vec{v})\right] \le \mathbb{E}_{\vec{v}\leftarrow D}\left[(\varphi_i(v_i)/\alpha - k_i + r_i)\cdot X_i(\vec{v})\right].$$

□

Proof of Lemma 7.2. Starting from Lemma A.2, we get the following chain of inequalities (letting $r := r(D_0)$ for simplicity of notation):

$$\begin{aligned}
p\cdot \Pr_{v\leftarrow D_0}[v\ge p] &\le p\cdot \Pr_{v\leftarrow D_0}[v\ge r]\cdot\left(\frac{r}{(1-\alpha)p+\alpha r}\right)^{\frac{1}{1-\alpha}}\\
&= r\cdot \Pr_{v\leftarrow D_0}[v\ge r]\cdot (p/r)\cdot\left(\frac{r}{(1-\alpha)p+\alpha r}\right)^{\frac{1}{1-\alpha}}\\
&\le r\cdot \Pr_{v\leftarrow D_0}[v\ge r]\cdot (p/r)\cdot\left(\frac{r}{(1-\alpha)p}\right)^{\frac{1}{1-\alpha}}\\
&= r\cdot \Pr_{v\leftarrow D_0}[v\ge r]\cdot (1-\alpha)^{-\frac{1}{1-\alpha}}\cdot (p/r)\cdot\left(\frac{r}{p}\right)^{\frac{1}{1-\alpha}}\\
&= r\cdot \Pr_{v\leftarrow D_0}[v\ge r]\cdot (1-\alpha)^{-\frac{1}{1-\alpha}}\cdot\left(\frac{r}{p}\right)^{\frac{\alpha}{1-\alpha}}.
\end{aligned}$$

The final line completes the proof. □

C PROOF OF PROPOSITION 4.1

Proof of Proposition 4.1. When $\alpha = 1$, we can directly invoke Theorem 4.1. When $\alpha \in (0, 1)$, we will set $f(n, D) := \frac{r(D)}{1-\alpha}\cdot(2/\alpha)^{\frac{1-\alpha}{\alpha}}\cdot(1-\alpha)^{-\frac{1-\alpha}{\alpha}}$ for all n. We will use $r := r(D)$ and $k := f(n, D)$ for ease of notation.

When there is a single real buyer, observe that the only strategies for the auctioneer are to submit fake bids $x_1 < \ldots < x_m$ for some $m \ge 0$. When $m = 0$, the auctioneer is behaving honestly. In fact, even when $m = 1$, the auctioneer is essentially behaving honestly (but sub-optimally). Indeed, observe that if $m = 1$ and $v_1 < x_1$, the auctioneer gets non-positive revenue by concealing x_1 (because the fine exceeds $r(D)$). Similarly, if $v_1 > x_1$, the auctioneer should clearly reveal x_1. Therefore, the auctioneers best safe, reasonable deviation (once committed to x_1) is to always reveal, meaning the new auction is effectively a reserve at x_1.

We are left to consider the case where $m \ge 2$. Using this same reasoning, we further observe that the auctioneer's best safe, reasonable deviation will never submit a fake bid $x_1 < k(m-1)$. To see this, observe that having committed to x_1 is only possibly helpful in the case that $v \in [x_1, x_2)$. If $v < x_1$, then the auctioneer would certainly have preferred not to submit x_1. If $v > x_2$, then the auctioneer will reveal x_2 anyway, and x_1 doesn't help. If $x_1 < k(m-1)$, however, then the auctioneer would rather reveal $x_2, \ldots, x_m$ and avoid fines ($k(m-1)$) than sell the item at x_1 ($< k(m-1)$). Therefore, we may assume w.l.o.g. that $x_1 \ge k(m-1) \ge k$.

Subject to this, it is now clear that the auctioneer's best safe, reasonable deviation, after committing to $x_1, \ldots, x_m$ is to reveal *all* x_i's whenever $v < x_1$ (otherwise, the fines greatly exceed $r(D)$). If $v \geq x_1$, then it is best to reveal x_i whenever $v \geq x_i$ and conceal x_i otherwise. In particular, this means that the auctioneer gets revenue only when $v \geq x_1 \geq k$, and their revenue when this occurs is clearly at most the buyer's value. We therefore conclude that for any strategy $x_1, \ldots, x_m$, the seller's expected payoff is at most $\mathbb{E}_{v \leftarrow D}[v \cdot I(v \geq k)]$. Our final task is just to upper bound this quantity. We first quickly observe that:

$$\begin{aligned}\mathbb{E}_{v \leftarrow D}[v \cdot I(v \geq k)] &= \int_0^\infty \Pr_{v \leftarrow D}[v \cdot I(v \geq k) > x]dx \\ &= \int_0^k \Pr_{v \leftarrow D}[v > k]dx + \int_k^\infty \Pr_{v \leftarrow D}[v > x]dx \\ &= k \cdot \Pr_{v \leftarrow D}[v > k] + \int_k^\infty \Pr_{v \leftarrow D}[v > x]dx.\end{aligned}$$

We now bound both terms. To bound the integral, we first use Lemma A.2 and observe $k \geq r$.

$$\begin{aligned}\int_k^\infty \Pr_{v \leftarrow D}[v > x]dx &\leq \Pr_{v \leftarrow D}[v \geq r] \cdot \int_k^\infty \left(\frac{r}{\alpha r + (1-\alpha)x}\right)^{\frac{1}{1-\alpha}} dx \\ &= \Pr_{v \leftarrow D}[v \geq r] \cdot \left[\frac{-(1-\alpha)}{\alpha} \cdot \left(\frac{r}{\alpha r + (1-\alpha)x}\right)^{\frac{\alpha}{1-\alpha}} \cdot \frac{r}{1-\alpha}\right]_{x=k}^{x=\infty} \\ &= \Pr_{v \leftarrow D}[v \geq r] \cdot \frac{r}{\alpha} \cdot \left(\frac{r}{\alpha r + (1-\alpha)k}\right)^{\frac{\alpha}{1-\alpha}} \\ &\leq \mathsf{Rev}(D) \cdot \frac{1}{\alpha} \cdot \left(\frac{r}{(1-\alpha)k}\right)^{\frac{\alpha}{1-\alpha}} \\ &\leq \mathsf{Rev}(D) \cdot \frac{1}{\alpha} \cdot \frac{\alpha}{2} = \mathsf{Rev}(D)/2.\end{aligned}$$

Above, the first step is due to Lemma A.2, and the last step is due to our particular choice of $k \geq \frac{r(D)}{1-\alpha} \cdot (2/\alpha)^{\frac{1-\alpha}{\alpha}}$. The intermediate steps are algebraic manipulation. To bound $k \cdot \Pr_{v \leftarrow D}[v > k]$, we directly use Lemma 7.2:

$$\begin{aligned}k \cdot \Pr_{v \leftarrow D}[v > k] &\leq r \cdot \Pr_{v \leftarrow D}[v \geq r] \cdot (1-\alpha)^{-1/(1-\alpha)} \cdot (k/r)^{-\alpha/(1-\alpha)} \\ &\leq r \cdot \Pr_{v \leftarrow D}[v \geq r] \cdot (1-\alpha)^{-1/(1-\alpha)} \cdot ((2/\alpha)^{\frac{1-\alpha}{\alpha}} \cdot (1-\alpha)^{-\frac{1-\alpha}{\alpha}}/(1-\alpha))^{-\alpha/(1-\alpha)} \\ &= r \cdot \Pr_{v \leftarrow D}[v \geq r] \cdot (1-\alpha)^{-1/(1-\alpha)} \cdot \frac{\alpha}{2} \cdot (1-\alpha) \cdot (1-\alpha)^{\frac{\alpha}{(1-\alpha)}}. \\ &= r \cdot \Pr_{v \leftarrow D}[v \geq r] \cdot \frac{\alpha}{2} \\ &\leq \mathsf{Rev}(D)/2.\end{aligned}$$

Again, the first step is a direct application of Lemma 7.2, and the last step is our particular choice of $k = \frac{r(D)}{1-\alpha} \cdot (2/\alpha)^{\frac{1-\alpha}{\alpha}} \cdot (1-\alpha)^{-\frac{1-\alpha}{\alpha}}$. Putting both bounds together, we see that the revenue of any safe, reasonable deviation is at most $\mathsf{Rev}(D)$, so therefore it is the seller's best response to be honest. $\square$

D EXAMPLE: DRA ON HEAVY TAIL DISTRIBUTIONS

Proposition D.1. *There exists a regular distribution D with unbounded expected value, such that for bounded $f(n, D)$,* DRA(f) *is optimal, strategyproof and computationally ε-credible, for some $0 < \varepsilon < 1$, when there is a single (real) buyer from D.*

Proof. We will define D such that even though it has infinite expected value, the tail of D is not too heavy so that with a finite fine we can limit the revenue the auctioneer can obtain. We will use $k := f(n, D) = e^e$ for ease of notation.

Let's first define an extension of tetration for positive real numbers.

$$h(x) := \begin{cases} 1 + x & \text{, for } -1 < x \leq 0 \\ e^{h(x-1)} & \text{, for } x > 0 \end{cases}$$

This function is continuous and differentiable in $(-1, \infty)$ ([Hoo06] for a detailed analysis of ultra exponential functions). Differentiating with respect to x,

$$h'(x) = \begin{cases} 1 & \text{, for } -1 < x \leq 0 \\ h(x)h'(x-1) & \text{, for } x > 0 \end{cases}$$

Define the natural super-logarithm $\ln^*(\cdot)$ to be the inverse of $h(\cdot)$. More formally, $\ln^*(x) = y$ if and only if $h(y) = x$ which implies the following property for every $x \in (0, \infty)$,

$$\ln^*(y) = \begin{cases} y - 1 & \text{for } 0 < y \leq 1 \\ 1 + \ln^*(\ln(y)) & \text{for } y > 1 \end{cases}$$

Observe that $\ln^*(e^x) = 1 + \ln^*(x)$ and $\ln^*(1) = 0$. Informally, one can interpret $\ln^*(x)$ as counting how many times one must take the natural-logarithm of x to get 1. We define the distribution D supported on $[1, \infty)$ in terms of the CDF:

$$Pr_{v \leftarrow D}[v > x] := \begin{cases} 1 & \text{, for } x \leq 1 \\ \frac{d}{dx} \ln^*(x) & \text{, for } x > 1 \end{cases}$$

By the chain rule, for $x > 1$, $Pr_{v \leftarrow D}[v > x] = \frac{1}{h'(\ln^*(x))}$. To see this is a valid distribution, observe $Pr_{v \leftarrow D}[v > x]$ is monotone decreasing, $Pr_{v \leftarrow D}[v > 1] = 1$, and $\lim_{n \to \infty} Pr_{v \leftarrow D}[v > n] = 0$. Now observe D has unbounded expected value:

$$\begin{aligned} E_{v \leftarrow D}[v] &= 1 + \int_1^{\infty} Pr_{v \leftarrow D}[X > x] dx \\ &= 1 + \lim_{n \to \infty} \ln^* n - \ln^* 1 = \infty \end{aligned}$$

For every safe and reasonable deviation, a buyer drawn from D receives $n \geq 0$ commitments and the auctioneer reveals a subset of those commitments. If $n = 0$, the auctioneer's revenue is maximized by selecting the optimal reserve price. In the next claim, we show that for every price $p \in \mathbb{R}^+$, $pPr_{v \leftarrow D}[v > p] \leq 1$.

Claim D.1. *For all $p \in \mathbb{R}^+$, $pPr_{v \leftarrow D}[v \geq p] \leq 1$.*

Proof. If $p \leq 1$, then $pPr_{v \leftarrow D}[v \geq p] = p \leq 1$. For $p > 1$, $\ln^* p > 0$ and by the recursive definition of $h'(\cdot)$, we can expand $h'(\ln^* p)$:

$$\begin{aligned} Pr_{v \leftarrow D}[v > p] &= \frac{1}{h'(\ln^* p)} = \frac{1}{h(\ln^* p)h'(\ln^* p - 1)} \\ &= \frac{1}{ph'(\ln^* p - 1)} \\ &\leq \frac{1}{p} \end{aligned}$$

where the last inequality follows from the fact $(\ln^* p - 1) > -1$ and $h'(\ln^* p - 1) \geq 1$. □

From the previous work, we can set $r(D) = 1$ as the optimal reserve price on D since $Pr_{v \leftarrow D}[v > r(D)] = 1$. When there is a single bidder, the only strategy for the auctioneer is to submit fake bids $x_1 < \ldots < x_n$ for some $n \geq 0$. Observe the auctioneer will never submit $x_i < k(n-i)$ for $i \in [n-1]$. To see this, if $v < x_{i+1}$, the auctioneer pay at least $k(n-i)$ as a fine for concealing all $x_j > v$. If $v \geq x_{i+1}$, the auctioneer will reveal x_{i+1} anyway, and x_i doesn't help. It follows, the optimal strategy is to reveal everything if $v < x_1$. If $v \geq x_1$, the auctioneer reveal x_i whenever $x_i \leq v$ and conceal otherwise. By Claim D.1, the auctioneer can obtain at most revenue L when it submits L commitments:

$$\begin{aligned} \sum_{i=1}^{L}(x_i - k(L-i))Pr_{v \leftarrow D}[v \in [x_i, x_{i+1})] &\leq \sum_{i=1}^{L} x_i Pr_{v \leftarrow D}[v \geq x_i] \\ &\leq L \end{aligned}$$

It follows, if the auctioneer obtains revenue at least 2, we have $n \geq 2$ which implies $x_1 \geq k(n-1) \geq n$ (for $k \geq e^e$). Now we bound the revenue when $v \in [0, e^n)$ using the fact the revenue $R(v)$ is at most v:

$$\begin{aligned} E_{v \leftarrow D}[R(v) \cdot I(0 \leq v < e^n)] &= E_{v \leftarrow D}[R(v) \cdot I(x_1 \leq v < e^n)] \\ &\leq E_{v \leftarrow D}[v \cdot I(n \leq v < e^n)] \\ &= \int_0^\infty Pr_{v \leftarrow D}[v \cdot I(n \leq v < e^n) > x]dx \\ &= \int_0^n Pr_{v \leftarrow D}[v \cdot I(n \leq v < e^n) > x]dx + \int_n^{e^n} Pr_{v \leftarrow D}[v \cdot I(n \leq v < e^n) > x]dx \\ &\quad + \int_{e^n}^\infty Pr_{v \leftarrow D}[v \cdot I(n \leq v < e^n) > x]dx \\ &\leq \int_0^n Pr_{v \leftarrow D}[n \leq v < e^n]dx + \int_n^{e^n} Pr_{v \leftarrow D}[v > x]dx + \int_{e^n}^\infty Pr_{v \leftarrow D}[n \leq v < e^n | v > x]dx \\ &\leq nPr_{v \leftarrow D}[v \geq n] + (\ln^*(e^n) - \ln^*(n)) + 0 \\ &\leq 1 + (1 + \ln^* n - \ln^* n) = 2 \end{aligned}$$

In the first line, we observe that if $v < x_1$, we have $R(v) = 0$. That's because the auctioneer can still charge $r(D) < k$ but it requires the auctioneer to conceal at least x_1. In second line, we simply observe $R(v) \leq v$. The fourth line is simply linearity of integration. In the sixth line, we observe $Pr_{v \leftarrow D}[v \cdot I(n \leq v < e^n) > x] = Pr_{v \leftarrow D}[v > x, n \leq v < e^n]$. In the seventh line, the first term follows by integrating the constant function in the interval 0 to n, the second term follows from the fundamental theorem of calculus, and the third term is 0 simply by observing the event

$\{n \leq v < e^n | v > x > e^n\} = \emptyset$. The last line follows by Claim D.1 and the recursive definition of super-logarithm.

Next we bound the revenue when $v > e^n$. Let $m = \min\{i : x_i \geq e^n\}$. For all $i \geq m$, when $v \in [x_i, x_{i+1})$, $R(v) = x_i$ which happens with probability at most $Pr_{v \leftarrow D}[v \geq x_i]$.

$$\begin{aligned}
E_{v \leftarrow D}[R(v) \cdot I(v \geq e^n)] &\leq \sum_{i=m}^{n} x_i Pr_{v \leftarrow D}[v \geq x_i] \\
&= \sum_{i=m}^{n} \frac{x_i}{h'(\ln^* x_i)} \\
&= \sum_{i=m}^{n} \frac{x_i}{x_i \ln x_i h'(\ln^* x_i - 2)} \\
&\leq \sum_{i=m}^{n} \frac{1}{nh'(\ln^* x_i - 2)} \\
&\leq \frac{n - m + 1}{n} \\
&\leq 1
\end{aligned}$$

The first equality follows by the definition of D. In the second equality, we use the fact $x_i \geq e^e$, which implies $h'(\ln^* x_i) = h(\ln^* x_i)h(\ln^* x_i - 1)h'(\ln^* x_i - 2) = x_i \ln x_i h'(\ln^* x_i - 2)$. In the third inequality, we use the fact $x_i \geq e^e$, which implies $h'(\ln^* x_i - 2) \geq 1$. We conclude the auctioneer can obtain revenue at most 3 when $f(n, D) = e^e$. □

E EXAMPLE: DRA ON α-STRONGLY REGULAR DISTRIBUTIONS

Definition E.1 (Almost reasonable). *A commitment is* loosely tied *to* $(m_1, r_1), \ldots, (m_k, r_k)$ *if the participant who sent c explicitly computed a poly-time function of* $c_1, \ldots, c_k$*, which were explicitly tied to* $(m_1, r_1), \ldots, (m_k, r_k)$*. A deviation is* almost reasonable *with respect to g for the auctioneer in the communication game if whenever the auctioneer reveals a commitment to c, with* $c = Commit(m, r)$*, then* $m = g(m_1, \ldots, m_k)$ *for some* $(m_1, r_1), \ldots, (m_k, r_k)$ *to which c is loosely tied.*

To help get intuition for the definition, observe that any reasonable deviation is also almost reasonable with respect to the identity function. If the commitment scheme is malleable, though, and it is possible to compute a poly-time function $g(\cdot, \ldots, \cdot)$ on un-revealed commitments, then a deviation which forwards a commitment to $g(b_1, \ldots, b_{n-1})$ to bidder n (before the commitments are revealed), and then later reveals $g(b_1, \ldots, b_{n-1})$ is almost reasonable with respect to g.

Definition E.2 (Strongly Computationally Credible). *An auction is* strongly computationally credible *with respect to g if, in expectation over* $\vec{v} \leftarrow D$*, and buyers being truthful, the auctioneer maximizes their expected revenue, over all deviations which are both safe and almost reasonable with respect to g, by executing the auction in earnest.*

An auction is strongly ε-computationally credible with respect to g if executing the auction in earnest yields a $(1 - \varepsilon)$*-fraction of the expected revenue of any safe, almost reasonable with respect to g, deviation.*

Theorems E.1 and E.2 below show that, perhaps surprisingly, both assumptions of unbounded distributions and non-malleable commitment schemes are necessary for Theorem 4.2 (whereas they were not necessary for Theorem 4.1, and appear to be just a technical artifact of our proof approach through Lemma 7.3).

Theorem E.1. *Let g be any function such that $g(m_1, \ldots, m_k) \geq max_{i\in[k]}\{m_i\}$. Then for all $\alpha < 1$, there exists a D_0 which is α-strongly regular, such that for all $\varepsilon > 0$ and all $f(\cdot,\cdot)$, there exists a sufficiently large n such that* DRA(f) *is not strongly $(1-\alpha-\varepsilon)$-computationally credible with respect to g for the instance $D := \times_{i=1}^{n} D_0$.*

In Theorem E.2 below, by the notation D_0^T, we mean the distribution D_0 *truncated at T* (all probability mass above T is moved to T. Formally, $\Pr_{v\leftarrow D_0}[v \geq x] = \Pr_{v\leftarrow D_0^T}[v \geq x]$ for all $x \leq T$, and $\Pr_{v\leftarrow D_0^T}[v \geq x] = 0$ for all $x > T$).

Theorem E.2. *For all $\alpha < 1$, there exists a distribution D_0 which is α-strongly regular, such that for all $\varepsilon > 0$ and all $f(\cdot,\cdot)$ such that $f(n, D)$ depends on $\alpha, \varepsilon, r(D), n$ (but may depend arbitrarily on these values), there exists a sufficiently large T and n such that* DRA(f) *is not $(1-\alpha-\varepsilon)$-credible for the instance $D := \times_{i=1}^{n} D_0^T$.*

The proofs of Theorems E.1 and E.2 will be nearly identical, and just wrap up differently at the end. Specifically, the D_0 for both theorems is the same, and the deviations are the same in spirit. First, we repeat the D_0 we use, which is the same from the proof of Theorem 4.4, repeated below for completeness:

$$F^{\alpha}(v) = \begin{cases} 0 & , v < 1 \\ 1 - \left(\frac{1}{v}\right)^{\frac{1}{1-\alpha}} & , v \geq 1 \end{cases} \qquad f^{\alpha}(v) = \begin{cases} 0 & , v < 1 \\ \frac{1}{1-\alpha}\left(\frac{1}{v}\right)^{\frac{2-\alpha}{1-\alpha}} & , v \geq 1 \end{cases}$$

The hazard rate of F^{α} is $h^{F^{\alpha}}(v) = \frac{1}{(1-\alpha)v}$ for $v \geq 1$ and the virtual value function of F^{α} is $\varphi^{F^{\alpha}}(v) = v - \frac{1}{h^{F^{\alpha}}(v)} = \alpha v$, so D_0 is α-strongly regular.

Our proof will proceed as follows. First, we will quickly establish that $\text{Rev}(D) = \alpha \cdot \mathbb{E}_{\vec{v}\leftarrow D}[\max_i\{v_i\}]$. Then, we will design a deviation which achieves revenue arbitrarily close to $\mathbb{E}_{\vec{v}\leftarrow D}[\max_i\{v_i\}]$ for sufficiently large n. Finally, we will show that this deviation satisfies the properties of the two theorems (separately).

Claim E.1. *For any n, and $D := D_0^n$, $Rev(D) = \alpha \cdot \mathbb{E}_{\vec{v}\leftarrow D}[max_i\{v_i\}]$.*

Proof. This could be verified by direct (but tedious) calculations. A simpler proof observes that $\text{Rev}(D) = \mathbb{E}[\max_i\{\varphi(v_i)\}]$ by Myerson's lemma. But because $\varphi(v_i) := \alpha v_i$, we immediately get that $\text{Rev}(D) = \mathbb{E}[\max_i\{\varphi(v_i)\}] = \alpha \cdot \mathbb{E}[\max_i\{v_i\}]$. □

Now, consider the following deviation in DRA(f). For any desired parameter δ, we will argue that the following deviation gets revenue (not counting fines) at least $(1-5\delta)\cdot\mathbb{E}[\max_i\{v_i\}]$, and also pays at most poly$(1/\delta)$ fines. Importantly, *the number of fines paid will depend only on δ and is independent of n* (it is not crucial that it is polynomial in $1/\delta$).

Our deviation is as follows: for $i = 0$ to z, where $z := (1-\alpha)\cdot\ln_{1+\delta}(1/(\alpha\delta))$, let $x_\ell := \delta\cdot(1+\delta)^{\ell}\cdot n^{1-\alpha}$. Upon receiving commitments to $b_1, \ldots, b_n$ from the bidders, the auctioneer will send to bidder i:

- A commitment to x_ℓ, for all ℓ.
- A single additional commitment to y_i^*, where it is guaranteed that $b_i > y_i^*$ *only if* $b_i > b_j$ for all $j \neq i$ (but perhaps $b_i \leq y_i^*$ for all i, this is also fine). Note that we defer to the last step of each proof exactly how to accomplish this for the two theorems of interest.

Next, the auctioneer will reveal commitments as follows:

- To all bidders $j \neq \arg\max_i\{b_i\}$, reveal all commitments. Note that this guarantees that bidder j does not expect to win the item.
- To bidder $i^* := \arg\max_i\{b_i\}$:
  - If $b_{i^*} < x_0$, reveal all commitments.
  - If $b_{i^*} > x_z$, reveal all commitments except $y_{i^*}^*$.

– If $b_{i^*} \in [x_\ell, x_{\ell+1})$, reveal commitments $x_0, \dots, x_\ell$ and conceal the rest.

Now, we analyze the revenue of this deviation *excluding fines*. We first need a quick observation about the relationship between $n^{1-\alpha}$ and $\mathbb{E}[\max_i\{v_i\}]$.

Observation E.1. $\mathbb{E}[\max_i\{v_i\}] \geq (1-1/e)n^{1-\alpha}$.

Proof. Observe that $\Pr[\max_i\{v_i\} > n^{1-\alpha}] \geq (1-1/e)$ (because each v_i exceeds $n^{1-\alpha}$ independently with probability exactly $1/n$). Therefore, $\mathbb{E}[\max_i\{v_i\}] \geq (1-1/e)n^{1-\alpha}$. □

Lemma E.1. *Excluding fines, the deviation above guarantees revenue at least* $(1-5\delta)\cdot\mathbb{E}[\max_i\{v_i\}]$ *in expectation.*

Proof. Observe first that the payment made by bidder i^* is:

- At least 0, when $v_{i^*} \notin [x_0, x_z]$.
- At least $(1-\delta)\cdot v_{i^*} \in [x_0, x_z]$.

This is just because payments (excluding fines) are always non-negative, and because whenever $v_{i^*} \in [x_0, x_z]$, there is always a revealed commitment within $(1-\delta)\cdot v_{i^*}$. So our only task is to argue that $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} \in [x_0, x_z])] \geq (1-4\delta)\cdot\mathbb{E}[\max_i\{v_i\}]$.

To do this, we will simply argue that the welfare lost from cases where $v_{i^*} < x_0$ is at most $2\delta\cdot\mathbb{E}[\max_i\{v_i\}]$, and also that the welfare lost from cases where $v_{i^*} > x_z$ is at most $2\delta\cdot\mathbb{E}[\max_i\{v_i\}]$.

Observation E.2. $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} < x_0)] \leq 2\delta\cdot\mathbb{E}[\max_i\{v_i\}]$.

Proof. Simply observe that $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} < x_0)] \leq x_0 = \delta n^{1-\alpha} \leq \frac{e}{e-1}\cdot\delta\cdot\mathbb{E}[\max_i\{v_i\}]$. □

Lemma E.2. $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} > x_z)] \leq 2\delta\cdot\mathbb{E}[\max_i\{v_i\}]$.

Proof. The lemma will follow from a few observations. First, we observe that $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} > x_z)] \leq \mathbb{E}[\sum_i v_i \cdot I(v_i > x_z)] = n\cdot\mathbb{E}[v_1\cdot I(v_1 > x_z)]$. Next, we observe that $n\cdot\mathbb{E}[v_1\cdot I(v_1 > x_z)] = n\cdot x_z\cdot(1-F^\alpha(x_z))/\alpha$. This could be observed by direct (but tedious) calculations. Alternatively, it follows as the expected revenue of setting price x_z to bidder one is exactly $x_z\cdot(1-F^\alpha(x_z))$, but also $\alpha\cdot\mathbb{E}[v_1\cdot I(v_1 > x_z)]$ by Myerson's lemma (and that $\varphi(v) = \alpha v$).

Now, our job is just to upper bound $x_z\cdot(1-F^\alpha(x_z))$. Recalling the definition of $F^\alpha(\cdot)$, this is exactly $x_z^{1-\frac{1}{1-\alpha}} = x_z^{-\frac{\alpha}{1-\alpha}}$. But now we get:

$$
\begin{aligned}
x_z^{-\frac{\alpha}{1-\alpha}} &= (n^{1-\alpha}\cdot(1+\delta)^z)^{-\frac{\alpha}{1-\alpha}} \\
&= n^{-\alpha}\cdot(1+\delta)^{-\frac{\frac{(1-\alpha)\cdot\ln_{1+\delta}(1/(\alpha\delta))}{\alpha}\cdot\alpha}{1-\alpha}} \\
&= n^{-\alpha}\cdot(1+\delta)^{-\ln_{1+\delta}(1/(\alpha\delta))} \\
&= n^{-\alpha}\cdot\alpha\cdot\delta.
\end{aligned}
$$

Finally, we now conclude that:

$$
\begin{aligned}
n\cdot x_z\cdot(1-F^\alpha(x_z))/\alpha &= n\cdot n^{-\alpha}\cdot(\alpha\delta)/\alpha \\
&= \delta n^{1-\alpha}.
\end{aligned}
$$

Again by Observation E.1, this is now at most $2\delta\mathbb{E}[\max_i\{v_i\}]$. □

Now, this concludes the proof of Lemma E.1. We have just argued that $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} < x_0)] \leq 2\delta\cdot\mathbb{E}[\max_i\{v_i\}]$, and also that $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} > x_z)] \leq 2\delta\cdot\mathbb{E}[\max_i\{v_i\}]$. Therefore, $\mathbb{E}[\max_i\{v_i\}\cdot I(\max_i\{v_i\} \in [x_0, x_z])] \geq (1-4\delta)\cdot\mathbb{E}[\max_i\{v_i\}]$, and the lemma follows as $(1-\delta)\cdot(1-4\delta) \geq (1-5\delta)$. □

Lemma E.1 argues that the revenue *excluding fines* of the above deviation is large. But we must now argue that the fines paid are small.

Lemma E.3. *The total fines paid by the above deviation is at most $z \cdot f(z+2, D_0)$. Importantly, observe that this is* independent of *n.*

Proof. The total number of commitments sent to each player is $z+1$. So including theirself, each player believes there are only $z+2$ bidders, and fines are computed accordingly. To each player, the auctioneer then clearly pays at most z fines when they conceal commitments (because they send only $z+1$, and reveal at least one when they hide any). □

We can now wrap up the proofs of Theorems E.1 and E.2.

Proof of Theorem E.1. To implement the proposed deviation, simply set $y_i^* = g(\vec{b}_{-i})$. By definition of g, this guarantees that $y_i^* > b_i$ for all $i \neq i^*$. For a given ε, first set $\delta < \varepsilon/100$ and use the proposed deviation. This guarantees revenue (including fines) of at least $(1-\varepsilon/2) \cdot \mathbb{E}[\max_i\{v_i\}] - z \cdot f(z+2, D_0)$. Because $z \cdot f(z+2, D_0)$ *is independent of n*, and D_0 is unbounded, there exists a sufficiently large n such that $z \cdot f(z+2, D_0) \leq (\varepsilon/2) \cdot \mathbb{E}[\max_i\{v_i\}]$. This completes the proof. □

Proof of Theorem E.2. Consider D_0^T for T to be set later, and define $D^T := \times_{i=1}^n D_0^T$. To implement the proposed deviation, simply set $y_i^* = T+1$. For a given ε, first set $\delta < \varepsilon/100$ and then use the proposed deviation. This guarantees revenue (including fines) of at least $(1-\varepsilon/3) \cdot \mathbb{E}_{\vec{v} \leftarrow D^T}[\max_i\{v_i\}] - z \cdot f(z+2, D_0^T) = (1-\varepsilon/3) \cdot \mathbb{E}_{\vec{v} \leftarrow D_0^T}[\max_i\{v_i\}] - z \cdot f(z+2, D_0)$. Note that the last equality follows as we have assumed that $f(k, D)$ depends only on $k, \varepsilon, \alpha, r(D)$, and $r(D) = r(D_0) = 1$. But now because $z \cdot f(z+2, D_0)$ *is independent of n*, and D_0 is unbounded, there exists a sufficiently large n and T such that $z \cdot f(z+2, D_0) \leq (\varepsilon/3) \cdot \mathbb{E}_{\vec{v} \leftarrow D^T}[\max_i\{v_i\}]$, and also that $\mathbb{E}_{\vec{v} \leftarrow D^T} \geq (1-\varepsilon/3) \cdot \mathbb{E}_{\vec{v} \leftarrow D}[\max_i\{v_i\}]$. This completes the proof. □

Finally, we show that Theorems E.1 and E.2 are tight. In the proof of Theorem E.3 below, note that Lemma 6.1 and Corollary 7.1 only require that β_i is a function of $\vec{b}_{-i}$, and not that it takes a particular (non-malleable) form.

Theorem E.3. *Let $f(n, D_i) := r(D_i)$. Then when all D_i are α-strongly regular (bounded or unbounded), DRA(f) is optimal, strategyproof, computationally $(1-\alpha)$-credible, and strongly computationally $(1-\alpha)$-credible with respect to all functions g.*

Proof. Let $k_i = r(D_i)$. Recall $X_i(\vec{v})$ is the indicator variable for the event where the item is allocated to buyer i and $k_i \leq v_i < \beta_i$. Also observe that $\bar{\phi}_i(v_i) = \phi_i(v_i)$ since D_i is regular. If $X_i(\vec{v}) = 1$, then $v_i \geq k_i \geq r_i$ and by definition $\phi_i(v_i) \cdot X_i(\vec{v}) \geq 0$. We first combine Lemma 6.1 and

Corollary 7.1:

$$\begin{aligned}
\mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v})] &= \mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v}) \cdot I(\exists\, i, v_i > \beta_i)] + \mathbb{E}_{\vec{v}\leftarrow D}[R(\vec{v}) \cdot I(\forall\, i, v_i < \beta_i)] \\
&\leq \mathbb{E}_{\vec{v}\leftarrow D}[\max_i\{\varphi_i(v_i)\} \cdot I(\exists\, i, v_i > \beta_i)] + \sum_{i=1}^{n} \mathbb{E}_{\vec{v}\leftarrow D}[(\varphi_i(v_i)/\alpha + r(D_i) - k_i) \cdot X_i(\vec{v})] \\
&\leq \mathbb{E}_{\vec{v}\leftarrow D}[\max_i\{\varphi_i(v_i)\}] + \sum_{i=1}^{n} \mathbb{E}_{\vec{v}\leftarrow D}[\varphi_i(v_i)/\alpha \cdot X_i(\vec{v})] - \mathbb{E}_{\vec{v}\leftarrow D}[\max_i\{\varphi_i(v_i)\} \cdot I(\forall i, v_i < \beta_i)] \\
&\leq \mathsf{Rev}(D) + \sum_{i=1}^{n} \mathbb{E}_{\vec{v}\leftarrow D}[\varphi_i(v_i)/\alpha \cdot X_i(\vec{v})] - \sum_{i=1}^{n} \mathbb{E}_{\vec{v}\leftarrow D}[\varphi_i(v_i) \cdot X_i(\vec{v}) \cdot I(\forall i, v_i < \beta_i)] \\
&\leq \mathsf{Rev}(D) + \sum_{i=1}^{n} \mathbb{E}_{\vec{v}\leftarrow D}[(1-\alpha)\varphi_i(v_i)/\alpha \cdot X_i(\vec{v})] \\
&\leq \mathsf{Rev}(D) + \frac{1-\alpha}{\alpha}\mathsf{Rev}(D) \\
&= \frac{1}{\alpha}\mathsf{Rev}(D)
\end{aligned}$$

The first line is just linearity of expectation. The second line combines Lemma 6.1 and Corollary 7.1. The third line is again by linearity of expectation and the fact $k_i = r(D_i)$. The fourth line uses the fact that $\mathbb{E}_{\vec{v}\leftarrow D}[\max_i\{\varphi_i(v_i)\}]$ is the revenue of Myerson's optimal auction and $\max(\varphi_i(v_i)) \geq \sum_{i=1}^{n} \varphi_i(v_i) \cdot X_i(\vec{v})$ since the indicator random variable $X_i(\vec{v}) = 1$ for at most one bidder. The fifth line is just the fact $X_i(\vec{v}) = 1$ implies $\forall i, v_i < \beta_i$ and by linearity of expectation. In the sixth line, we observe that the second term is at most the revenue of the second price auction.

This concludes that the revenue of any deviation which is safe, and almost reasonable *with respect to any* $g(\cdot)$, is at most $\mathsf{Rev}(D)/\alpha$.

□