Credible, Truthful, Bounded-round Mechanisms with commitments: Overview and a first-analysis

MATTEO RUSSO, MATHEUS V.X. FERREIRA, MATTHEW S. WEINBERG

In a seminal paper by Akbarpour and Li [1], they show that there is no mechanism which satisfies the properties of truthfulness, credibility and bounded-roundness. However, when bids are encrypted through commitment schemes, Ferreira and Weinberg [2] show that there exists a 2-round truthful, credible and optimal mechanism which fines the bidders (and potentially fictitious ones submitted by the auctioneer) in addition to the payment scheme. In our work, we prove that, in 1-round mechanisms, commitment schemes are of no use and, hence, Akbarpour and Li's result still holds. For what regards k-round mechanisms, with $k > 1$, we show that (not present in this first report) the *DRA* is the only k-round mechanism with the above properties along with realistic requirements our auction needs to possess.

1 1-ROUND MECHANISMS

1.1 Definitions and Preliminaries

Definition 1.1. Consider a set of m bidders competing for the purchase of a given item from an auctioneer in a mechanism with m bids in k rounds $\mathcal{M}(\boldsymbol{b}, k)$. A 1-round mechanism $\mathcal{M}(\boldsymbol{b}, 1)$ is defined to be the following communication game between bidders and auctioneer:

Round 1a. Bidders $\xrightarrow{\text{speak}}$ Auctioneer

Round 1b. Auctioneer $\xrightarrow{\text{speak}}$ Bidders

Definition 1.2. Consider a set of m bidders competing for the purchase of a given item from an auctioneer in any k-round mechanism $\mathcal{M}(\cdot, k)$. For bids represented in β bits $b \in \{0,1\}^{\beta}$ and pads represented in ρ bits $r \in \{0,1\}^{\rho}$, let us define commitment scheme what follows:

$$\text{Commit}(\boldsymbol{b}, \boldsymbol{r}) := \left(g^{b} h^{r}\right)_{b \in \boldsymbol{b}, r \in \boldsymbol{r}}$$

whereby, $\boldsymbol{b} \sim \bigtimes_{i \in [m]} D_i$ and $\boldsymbol{r} \sim U_{\rho}^{m}$, which denotes the m-dimensional uniform distribution on ρ representation bits. Commit$(\cdot,\cdot)$ follows the Pedersen scheme, that is the above expression where g is the generator of a group of prime order under which the discrete logarithm is (believed to be) hard. Every potential receiver of a message raises g to a random power to get another generator h, and publicly announces h.

Definition 1.3 (Equivalent bids classes). Let us denote by $\mathcal{Y} = \bigtimes_{j \in [m]} \text{supp}\left(D_j\right)$ and by $\mathcal{Y}_{-i} = \bigtimes_{j \in [m] \setminus \{i\}} \text{supp}\left(D_j\right)$. Consider two bids $b_i, b_i' \in \text{supp}\left(D_i\right)$, we will say that two bids are not equivalent if there exists some profile of other bids such that one of b_i, b_i' wins and the other one loses and equivalent otherwise. Formally, b_i belongs to same equivalence class of b_i', name it C_i, if the following statement holds:

$$b_i, b_i' \in C_i \ \text{ if and only if } \ \boldsymbol{x}_i\left(b_i, \boldsymbol{b}_{-i}\right) = \boldsymbol{x}_i\left(b_i', \boldsymbol{b}_{-i}\right), \ \forall\, \boldsymbol{b}_{-i} \in \mathcal{Y}_{-i} \tag{1}$$

We can, thus, express an equivalence class with the following set notation:

$$C_i := \left\{b_i, b_i' \in \text{supp}\left(D_i\right) \middle| \boldsymbol{x}_i\left(b_i, \boldsymbol{b}_{-i}\right) = \boldsymbol{x}_i\left(b_i', \boldsymbol{b}_{-i}\right), \ \forall\, \boldsymbol{b}_{-i} \in \mathcal{Y}_{-i}\right\} \tag{2}$$

Example 1.4. Consider two bidders competing for the purchase of a given item in a 1-round mechanism $\mathcal{M}\left(\left(b_1, b_2\right), 1\right)$. Let $b_1 \in \operatorname{supp}\left(D_1\right) = \{1, 5\}$ and $b_2 \in \operatorname{supp}\left(D_2\right) = \{2, 4\}$ and suppose we allocate the item to the bidder with highest value. Then, following Definition 1.3, we are able to say that for bidder 1, 5 and 1 cannot be equivalent bids given that 5 will always be a winning bid and 1 always a losing one, no matter what bidder 2 decides to bid. For bidder 2, 2 and 4 are equivalent since both would lose against 5 or both would win against 1.

Given the above description of what a 1-round mechanism, commitment schemes and equivalence classes look like, in the following simple proposition and observation, we establish that the auctioneer (whether honest or not) before announcing the bidder and the price to be paid has to know all bidders' values equivalence classes. Otherwise, it might be the case the the former is unable to assign the item to any of the bidders, a fallacy which is not usually allowed in an auction model.

1.2 Main results for 1-round mechanisms

Proposition 1.5. *Consider a set of m bidders competing for the purchase of a given item from an auctioneer in any 1-round revenue optimal mechanism $\mathcal{M}(\boldsymbol{b}, 1)$. Then, after round **1a**, the auctioneer must know all bidders' values equivalence classes with a point-mass Bayesian belief over a bid b_i for an equivalence class C_i and for all $i \in [m]$ of the form*

$$Pr\left[b_i \in C_i\right] \in \{0, 1\}$$

Proof. Assume for contradiction that the auctioneer has a non-point mass Bayesian belief over a message (bid) b_i membership to equivalence classes. This implies that there exist two equivalence classes such that bidder i could have sent their message (bid) from both classes, meaning that there is a positive probability that the message (bid) belongs to either of the classes. Formally, this means that for equivalence classes $\mathcal{A}_i, \mathcal{B}_i$, with $\mathcal{A}_i \neq \mathcal{B}_i$,

$$\Pr\left[b_i \in \mathcal{A}_i\right] \in (0, 1)$$
$$\Pr\left[b_i \in \mathcal{B}_i\right] \in (0, 1)$$

Then, there exists a bid profile $\boldsymbol{b}_{-i}$ for the remaining bidders such that the following holds:

$$\Pr\left[\boldsymbol{x}_i\left(b_i, \boldsymbol{b}_{-i}\right) = 0 | b_i \in \mathcal{A}_i\right] > 0$$
$$\Pr\left[\boldsymbol{x}_i\left(b_i, \boldsymbol{b}_{-i}\right) = 1 | b_i \in \mathcal{B}_i\right] > 0$$

Hereby, $\mathcal{A}_i$ is the winning equivalence class and $\mathcal{B}_i$ is a losing equivalence class. By the probabilistic method, this implies that there exists a positive probability event such that the message (bid) b_i belongs to winning equivalence class $\mathcal{A}_i$ and the item is not allocated to bidder i and for which the message (bid) b_i belongs to losing equivalence class $\mathcal{B}_i$, and the item is allocated to bidder i, which is a contradiction. The statement of the proposition is thus proved, as desired. □

Given that, by Proposition 1.5, the auctioneer must know all bidders' values equivalence classes by round **1a**, then, we would like to formally establish a claim where we conclude that, in 1-round truthful and optimal mechanisms, commitment schemes are of no use, which means that this type of mechanism is never credible. In other words, the auctioneer, after having learnt the bidders' equivalence classes, could simply pretend that everyone has bid in the equivalence class immediately below the winning one and the mechanism would still be consistent from the bidders' perspective, as stated in Observation 1.6 below.

Observation 1.6. Consider a set of m bidders competing for the purchase of a given item from an auctioneer in any 1-round truthful and optimal mechanism with commitments $\mathcal{M}(\boldsymbol{c}, 1)$. Then, $\mathcal{M}(\boldsymbol{c}, 1)$ is not credible.

Proof. By Proposition 1.5, the auctioneer knows all bidders' equivalence classes by the end of round **1a**. We, thus, need to construct a counterexample of distributions for which the truthful and optimal auction using commitments cannot be credible. Consider two bidders both uniformly distributed on the interval $[0,1]$, that is $v_1, v_2 \sim U_{[0,1]}$, competing in a second-price auction with commitments and reserve price $1/2$. We first note that the second-price auction is truthful and the reserve price of $1/2$ for this distribution makes the auction also revenue optimal. Moreover, any value between $1/2$ and 1 is in its own equivalence class. Indeed, consider values for bidder 1 $v_1, v_1' \in [1/2, 1]$, with $v_1 < v_1'$: then, they cannot be in the same equivalence class because, supposing for instance that bidder 2 has value $v_2 = (v_1 + v_1')/2$, then v_1 would lose against v_2 with probability 1 and v_1' will win against v_2 with probability 1. Thus, for bidder $i \in \{1, 2\}$, the equivalence classes are $C_i^{(0)}$ for all those v_i 's such that $v_i < 1/2$ as well as $C_i^{(y_i)}$ for each $y \in [1/2, 1]$ as argued before. Hence, we have the following three cases where we need to show why a deviating auctioneer earns more in expectation if compared to an honest one:

Case 1. With probability $1/4$, both $v_1 \in C_1^{(0)}$ and $v_2 \in C_2^{(0)}$. Then, the item is not allocated and the auctioneer has revenue equal to 0. In this case, there does not exist a strategy yielding higher revenue than being honest, as it would require the auctioneer to sell the item for less than $1/2$, which is not optimal. Thus, the honest and the deviating auctioneer have both revenue equal to 0.

Case 2. With probability $1/4$, both $v_1 \in C_1^{(y_1)}$ and $v_2 \in C_2^{(y_2)}$, for some $y_1, y_2 \in [1/2, 1]$. Then, in this case, the expected revenue for the honest auctioneer is the expectation over the interval $[1/2, 1]$ of the second highest value, which for uniformly random variables, is $2/3$. For what concerns the deviating auctioneer, assume without loss of generality that $y_1 < y_2$. Then, the auctioneer could create a fictitious equivalence class $C_1^{(z)}$, with $y_1 < z < y_2$, and obtain expected revenue strictly greater than $2/3$, whilst being consistent with the auction format.

Case 3. With probability $1/2$, either $v_1 \in C_1^{(0)}$ and $v_2 \in C_2^{(y_2)}$, for some $y_2 \in [1/2, 1]$ or $v_1 \in C_1^{(y_2)}$ and $v_2 \in C_2^{(0)}$, for some $y_1 \in [1/2, 1]$. Then, in this case, the expected revenue for the honest auctioneer is the reserve price, that is $1/2$. For what concerns the deviating auctioneer, assume, without loss of generality, that we are in the case for which $v_1 \in C_1^{(0)}$. Then, the auctioneer could create a fictitious equivalence class $C_1^{(z)}$, with $1/2 \leq z < y_2$, and obtain expected revenue strictly greater than $1/2$, whilst being consistent with the auction format.

In a truthful and optimal mechanism like $\mathcal{M}(\boldsymbol{c}, 1)$, the honest auctioneer would get expected revenue equal to $5/12$, whereas the deviating one an expected revenue strictly greater than $5/12$. Thus, $\mathcal{M}(\boldsymbol{c}, 1)$ is not credible. □

In addition to Observation 1.6 above, we are even able to assert a stronger result, namely that any auction that the auctioneer can implement in one round with commitments, they can also implement in one round without commitments. The idea behind the technical proof of Lemma 1.7 is that every committed bid is either not revealed in the first round or it is indeed revealed in the first round. In the former case, the committed bid is never revealed, and, by perfect hiding, the auctioneer cannot use it at all to determine the winner and the payment amount. In the latter case, bidders are committing to their bid to then reveal it in the same round, which simply reduces to not committing in the first place. We, thus, conclude that every 1-round mechanism with commitments is equivalent to a corresponding 1-round mechanism without commitments.

Lemma 1.7 (Commitment schemes in 1-round mechanisms). *Consider a set of m bidders competing for the purchase of a given item from an auctioneer in any 1-round mechanism $\mathcal{M}(\cdot, 1)$. For bids* *represented in β bits $b \in \{0,1\}^{\beta}$ and pads represented in ρ bits $r \in \{0,1\}^{\rho}$, let*

$$\boldsymbol{c} := Commit(\boldsymbol{b}, \boldsymbol{r}) \text{ and } \boldsymbol{c}' := Commit(\boldsymbol{b}', \boldsymbol{r}')$$

whereby $\boldsymbol{b}, \boldsymbol{b}' \overset{\text{i.i.d.}}{\sim} \bigtimes_{i \in [m]} D_i$ and $\boldsymbol{r}, \boldsymbol{r}' \overset{\text{i.i.d.}}{\sim} U_{\rho}^{m}$, which denotes the m-dimensional uniform distribution on ρ representation bits. Denote by $\mathcal{M}(\boldsymbol{c}, 1)$ and by $\mathcal{M}(\boldsymbol{c}', 1)$ the distribution of mechanism $\mathcal{M}(\boldsymbol{c}, 1)$ outcomes for the two different committed bid vectors $\boldsymbol{c}, \boldsymbol{c}'$. Then, $\mathcal{M}(\boldsymbol{c}, 1)$ is truthful if and only if $\mathcal{M}(\boldsymbol{c}', 1)$ is, $\mathcal{M}$ is credible if and only if $\mathcal{M}(\boldsymbol{c}', 1)$ is and their distributions of outcomes are identical, that is

$$\mathcal{M}(\boldsymbol{c}, 1) = \mathcal{M}(\boldsymbol{c}', 1) \tag{3}$$

Proof. Showing that commitment schemes are not useful in a single round is equivalent to showing a reduction of any single round protocol where bidders send committed bids to another single round protocol where bidders do not send committed bids at all and where truthfulness and credibility of one mechanism imply truthfulness and credibility of the other. To this end, consider the mechanism $\mathcal{M}$, where an arbitrary bidder sends the committed bid $b \sim D$ with a one time uniformly random pad $r \sim U_{\rho}$, $c := \text{Commit}(b, r)$. We observe that the commitment has the same distribution as a random string (with the same size of the bid) given that it perfectly hides it by assumption (information theoretically it reveals nothing about b): in other words, $c \sim U_{\beta}$.

Given this single round mechanism, consider a second mechanism that executes exactly in the same manner as the first one except that when a bidder is requested to send c, they send a blank bid $(-)$ and the auctioneer replaces this blank bid $(-)$ by $c' := \text{Commit}(b', r')$, where $b' \sim D$ and $r' \sim U_{\rho}$ are chosen by the auctioneer independently of b and r.[1] We will now show why the distribution of an outcome $\omega \sim \mathcal{M}(c, 1)$ is equal to the distribution of another outcome $\omega' \sim \mathcal{M}(c', 1)$. Firstly, note that if $c := \text{Commit}(b, r)$ and $c' := \text{Commit}(b', r')$ were not identically distributed, then one could use this auctioneer as an oracle to distinguish c from c' which is impossible by the perfect hiding definition and the cryptographic primitives in use. Moreover, the mechanism computation on the auctioneer side could be seen as a function applied to the random variables c and c', that is $\omega := \mu(c)$ and $\omega' := \mu(c')$, where μ is the function corresponding to distribution $\mathcal{M}$. Since c and c' are identically distributed, so will be the obtained random variables ω and ω'. This means that, indeed, $\mathcal{M}(c, 1) = \mathcal{M}(c', 1)$. Insofar as the above reasoning has been applied to arbitrary components c, c' of vectors $\boldsymbol{c}, \boldsymbol{c}'$, we have that $\mathcal{M}(\boldsymbol{c}, 1) = \mathcal{M}(\boldsymbol{c}', 1)$, as desired. □

The proof of Lemma 1.7 hinges on the following two fundamental facts: the bidder sends exclusively the committed bid and the mechanism lasts only for a single round. The first remark below, in fact, demonstrates how the reduction outlined in the proof no longer holds for bidders sending their bid together with the commitment. The second remark in the next section, on the other hand, shows that the same happens if rounds are multiple and, thus, explains why not all k-round mechanisms where commitment schemes are used are equivalent to corresponding k-round mechanisms where commitment schemes are not used (with $k \geq 2$).

Remark 1.8 (Bids and Commitments). Let us note that, since (b, r) and (b', r') are independent and identically distributed by construction, the proof of Lemma 1.7 holds for random variables that keep this independence. Nevertheless, the distribution of $d := ((b, r), \text{Commit}(b, r))$ is not the same as the distribution of $d' := ((b, r), \text{Commit}(b', r'))$ because (b, r) is correlated with $\text{Commit}(b, r)$

[1] As a clarification, the bidders or the auctioneer might still use commitments on their respective sides but commitments are never exchanged between the bidder and the auctioneer, which means that the mechanism does not use commitment schemes.

and (b, r) is independent of $\mathtt{Commit}(b', r')$. Hence, we have $\mathcal{M}(d, 1) \neq \mathcal{M}(d', 1)$. As anticipated, Lemma 1.7 no longer holds for bidders sending their bid together with their committed bid.

Remark 1.9 (Multiple Rounds and Strawman Auction with Abort). Let us take $k = 2$ and consider the Strawman second-price auction where, if at least one bidder conceals, the mechanism aborts, the item does not get allocated and the auctioneer gets revenue 0. For short, we will name this auction format **Strawman Auction with Abort**. Let us set the reserve of this mechanism 1 and let us consider a single bidder whose value is uniformly distributed over $\{1, 2\}$. The auctioneer again can run two specular mechanisms $\mathcal{M}$ and $\mathcal{M}'$, where, in the first, they are not allowed to exchange commitments with the bidder and, in the second, they are.
In mechanism $\mathcal{M}$ with commitments, the auctioneer could be honest or could deviate by submitting a fake committed bid and, then, revealing or concealing it as convenient. In particular, the honest auctioneer gets expected revenue $\mathbb{E}\left[\mathrm{Rev}\left(\mathcal{M}\right)\right] = 1$, no matter what the bidder's value is. On the other hand, the deviating auctioneer could employ the following strategy: with probability π_ℓ, commit to one of n bids between 1 and 2 (both included), call them a_ℓ, $\ell \in [n]$, where $a_1 = 1$ and $a_n = 2$. Then, if the bidder's value is $v = 2$, which happens with probability $1/2$, in all cases, the auctioneer will reveal and get revenue a_ℓ. So, with probability $\pi_\ell/2$, the auctioneer gets value a_ℓ. When the bidder's value is $v = 1$, which also happens with probability $1/2$, then the auctioneer will conceal in $n - 1$ cases and reveal only when they had committed to 1. Thus, only with probability $\pi_1/2$, the auctioneer gets revenue 1. Thus, the deviating auctioneer's expected revenue is

$$\begin{aligned}\mathbb{E}\left[\mathrm{Rev}\left(\mathcal{M}, \boldsymbol{\pi}, \boldsymbol{a}\right)\right] &= \sum_{\ell\in[n]} \frac{\pi_\ell}{2} \cdot a_\ell + \frac{\pi_1}{2} \cdot 1 = \pi_1 + \sum_{\ell=2}^{n-1} \frac{\pi_\ell}{2} \cdot a_\ell + \pi_n \\ &\leq \pi_1 + \sum_{\ell=2}^{n-1} \frac{\pi_\ell}{2} \cdot 2 + \pi_n = \sum_{\ell\in[n]} \pi_\ell = 1 \\ &= \mathbb{E}\left[\mathrm{Rev}\left(\mathcal{M}\right)\right].\end{aligned}$$

This means that the mechanism $\mathcal{M}$ is credible since the honest auctioneer would have revenue greater than or equal to the deviating one.
Mechanism $\mathcal{M}'$ is the counterpart of $\mathcal{M}$ without commitments. In other words, the **Strawman Second-Price Auction with Abort** without commitments reduces simply to a second-price auction with reserve 1, which is known not to be credible. We have shown that there exists a credible mechanism with commitments where the "without commitments" counterpart is not credible.
As a nota bene, the **Strawman Auction with Abort** is not an advantageous mechanism to implement in practice for the auctioneer, despite truthfulness and credibility. In fact, imagine an online platform where the trading of goods is regulated by the **Strawman Auction with Abort**, then, a potential platform competitor could always submit and conceal the committed bid to make the competing platform crash all the time and the corresponding auctioneer have revenue 0.

The above considerations motivate why it is important to delve into the use of commitment schemes in k-rounds mechanisms (with $k \geq 2$), and understand the reason why they are the right tool to design credible, optimal and truthful bounded-round mechanisms both in theory and in practice.

2 2-ROUND MECHANISMS

2.1 Definitions and Preliminaries

Definition 2.1. Consider a set of m bidders competing for the purchase of a given item from an auctioneer in a mechanism with m bids in 2 rounds $\mathcal{M}(\boldsymbol{b}, 2)$. A 2-round mechanism $\mathcal{M}(\boldsymbol{b}, 2)$ is defined to be the following communication game between bidders and auctioneer:

Round 1a. Bidders $\xrightarrow{\text{speak}}$ Auctioneer

Round 1b. Auctioneer $\xrightarrow{\text{speak}}$ Bidders

Round 2a. Bidders $\xrightarrow{\text{speak}}$ Auctioneer

Round 2b. Auctioneer $\xrightarrow{\text{speak}}$ Bidders

The coming paragraphs will describe what sorts of mechanisms are allowed in our model and the reason why we decided to constrain it to a specific set of auctions. In particular, Remark 1.9 describes an auction in two rounds which uses commitment schemes and is indeed both truthful and credible. Nevertheless, the **Strawman Auction with Abort**, and for that matter, any mechanism of the form "if at least one bidder does not reveal by the second round, then, abort the auction", is impractical insofar as a competing auctioneer possessing another platform could simply commit to a bid in the first round and never reveal it in the second, making the competitor's platform always crash. We, thus, need to reduce the set of auctions we allow to consider within our model to the ones that follow Myerson's allocation rule only on revealed bids.

Allocation 2.2. Consider a set of m bidders competing for the purchase of a given item from an auctioneer in a mechanism with m bids in 2 rounds $\mathcal{M}(\boldsymbol{b}, 2)$. Moreover, consider a set of $n \leq m$ bidders that by round **2a** reveal their committed bid. The auctioneer applies the Myerson's allocation rule on the n revealed bids, where $\varphi_j\left(v_j\right)$ is the j^{th} bidder virtual value with $v_j \sim D_j$:

$$x_i\left(v_i, \boldsymbol{v}_{-i}\right) = 1 \iff i \in \arg\max_{j \in [n]} \varphi_j\left(v_j\right),\ \varphi_i\left(v_i\right) \geq 0$$

Below, we will see why it is fundamental to apply Myerson's allocation rule as well as other additional properties to guarantee an implementable mechanism in the real world which satisfies credibility, truthfulness and optimality in 2 rounds.

The only flexibility the auctioneer possesses is that of deciding on some payment scheme which is a function of the bidders values and the number of concealed bids $\mathsf{P} : \mathcal{Y} \times \mathbb{N} \longrightarrow \mathbb{R}$, $\mathsf{P}\left(v_i, \boldsymbol{v}_{-i}, m-n\right)$. The question is one of understanding whether the payment function exists, is unique or whether there are multiple payment functions that satisfy our model constraints. If so posed, there exist solutions to this question which are impractical and need to be ruled out in our final model.

Solution 2.3 (Impractical). Consider the following payment function for a 2-round mechanism with m bidders and letting, without loss of generality, bidder $i \in [m]$ be the winner of the auction:

$$\mathsf{P}\left(v_i, \boldsymbol{v}_{-i}, m-n\right) = \begin{cases} \max_{j \in [m] \setminus \{i\}} v_j, & \text{if } m-n=0 \\ 0, & \text{otherwise} \end{cases}$$

This is a second-price auction whenever no one conceals their own bid and it gives the item arbitrarily for free whenever someone conceals. Clearly, the auction is truthful, satisfies Myerson's allocation rule and is credible insofar as it is a **Strawman Auction with Abort** with no reserve price. For the same reason, the auction is impractical as some interested third party could always commit and conceal and the auctioneer would give the item for free to an arbitrary bidder, getting revenue equal to 0.

The impractical Solution 2.4 and Allocation 2.2 immediately and naturally delineate two fundamental properties that our model should possess:

Property I. The auctioneer has to assign the item to the bidder corresponding to the highest virtual value, which is guaranteed by Myerson's allocation rule.

Property II. The auctioneer has to be paid an amount equal to Myerson's optimal auction revenue on revealed bids.

Surely, **Property I** rules out mechanisms that do not follow Myerson's allocation rule, which are problematic for the reasons outlined above. On the other hand, **Property II** rule out auctions such as Solution 2.4 or the **Strawman Auction with Abort** insofar as they do not necessarily obtain Myerson's optimal payment. Nevertheless, the two properties of above are not sufficient to construct a robust enough model to start from and to make considerations on as the following other impractical solution exemplifies.

Solution 2.4 (Impractical). Consider the following payment function for a 2-round mechanism with m bidders and n revealed bids. Letting, without loss of generality, bidder $i \in [m]$ be the winner of the auction and bidder 1 be the arbitrarily picked one by the auctioneer, with $i \neq 1$, we have that

$$\mathsf{P}\left(v_i, \boldsymbol{v}_{-i}, m-n\right) = \begin{cases} \bar{\varphi_i}^{-1}\left(\max\left\{0, \max_{j\in[m]\setminus\{i\}} \bar{\varphi_j}\left(v_j\right)\right\}\right), & \text{if } m-n=0 \\ 0, & \text{otherwise} \end{cases}$$

$$\mathsf{P}\left(v_1, \boldsymbol{v}_{-1}, m-n\right) = \begin{cases} 0, & \text{if } m-n=0 \\ \bar{\varphi_i}^{-1}\left(\max\left\{0, \max_{j\in[n]\setminus\{i\}} \bar{\varphi_j}\left(v_j\right)\right\}\right), & \text{otherwise} \end{cases}$$

In other words, if no one conceals, the auctioneer runs Myerson's auction with its allocation rule and payment scheme. On the contrary, if there is at least one concealed bid, the auctioneer picks one bidder arbitrarily and makes them pay me the Myerson's optimal revenue, while charging the actual winner 0. This type of auction is impractical insomuch as, in a real-world scenario, a bidder would likely conceal because the Internet connection drops down and it is, therefore, infeasible to collect from them, given that they are not on the platform any longer. Moreover, it would be unrealistic to expect an arbitrary bidder to pay unboundedly much (sometimes even beyond their true value) since such a bidder would never take the risk to be charged so much whilst not even receiving the item.

We have, thus, established that the mechanisms we are after need to run Myerson's allocation rule and payment scheme only on revealed bids in order to avoid the impractical corner solutions outlined above. In other words, **Property II** needs to be stronger in the sense not only does the auctioneer need to be paid an amount equal to Myerson's auction revenue on revealed bids but the payment scheme has to be exactly the same to Myerson's auction, thus, ensuring truthfulness, optimality as well as guaranteeing that impractical situations do not arise.

Model 2.5 (Truthful, Optimal and Practical 2-round mechanism). Consider a set of m bidders competing for the purchase of a given item from an auctioneer in a 2-round mechanism $\mathcal{M}(\boldsymbol{b}, 2)$ and let n be the number of revealed bids. $\mathcal{M}$ is characterized by the following allocation rule and payment scheme on revealed bids.

$$\boldsymbol{x}_i\left(v_i,\boldsymbol{v}_{-i}\right)=1 \iff i\in\arg\max_{j\in[n]}\varphi_j\left(v_j\right),\ \varphi_i\left(v_i\right)\geq 0$$

$$\mathsf{P}\left(v_i,\boldsymbol{v}_{-i},m-n\right)=\bar{\varphi_i}^{-1}\left(\max\left\{0,\max_{j\in[n]\setminus\{i\}}\bar{\varphi_j}\left(v_j\right)\right\}\right)$$

In other words, $\mathcal{M}$ is Myerson's optimal mechanism on revealed bids.

REFERENCES

[1] Mohammad Akbarpour and Shengwu Li. 2020. Credible Auctions: A Trilemma. *Econometrica* 88, 2 (March 2020), 425–467. https://doi.org/10.3982/ECTA15925

[2] Matheus V. X. Ferreira and S. Matthew Weinberg. 2020. Credible, Truthful, and Two-Round (Optimal) Auctions via Cryptographic Commitments. arXiv:cs.GT/2004.01598