Budget Imbalance Criteria for Auctions: A Formalized Theorem[*]

Marco B. Caminati[1], Manfred Kerber[1], and Colin Rowat[2]

[1] School of Computer Science, University of Birmingham, UK
[2] Economics, University of Birmingham, UK
Project homepage: `http://cs.bham.ac.uk/research/projects/formare/`

Abstract. We present an original theorem in auction theory: it specifies general conditions under which the sum of the payments of all bidders is necessarily not identically zero, and more generally not constant. Moreover, it explicitly supplies a construction for a finite minimal set of possible bids on which such a sum is not constant. In particular, this theorem applies to the important case of a second-price Vickrey auction, where it reduces to a basic result of which a novel proof is given. To enhance the confidence in this new theorem, it has been formalized in Isabelle/HOL: the main results and definitions of the formal proof are reproduced here in common mathematical language, and are accompanied by an informal discussion about the underlying ideas.

1 Introduction

The ForMaRE project [4] employs formal methods to provide a unified approach to both the generation of executable code for running auctions and the proving of theorems about them. In this paper, we will describe the formalization of a classical result about the second price Vickrey auction (which will be introduced in Section 2), stating that the sum of the payments for all participants cannot be zero for all possible bids. We will indicate this result as NB (for *no balance*).

The proof mechanism we present for NB is, to the best of our knowledge, new. Although it is also applicable to the specific case of the Vickrey auction, our proof works for a wide class of possible auction mechanisms: indeed, it gives a characterization of the kinds of auctions for which it holds. By contrast, all the existing proofs we know of vitally rely on the particular algebraic form that the mechanism assumes in the particular case of the Vickrey auction. Furthermore, our proof explicitly constructs a minimal, finite set of possible bids on which the sum of all the payments is not a constant function.

All the results have been formalized and checked in the Isabelle/HOL theorem prover [7]. Because the results are new, they are stated here in common mathematical language, which should be friendlier for the reader. The lemmas, definitions, and theorems in this paper correspond as far as possible their

---

formalized counterparts and for each statement we indicate the corresponding Isabelle name in typewriter font. The relevant Isabelle theory file is `Maskin3.thy`, available at `https://github.com/formare/auctions/`.

1.1 Structure of the paper

In Section 2, some context is given: we will see the basic mathematical definitions for auctions, which will be needed to state the main theorem NB, the object of the present formalization.

Section 3 informally illustrates the idea behind our original proof of NB, and Section 4 presents the formal result implementing this idea, which is Lemma 1. This lemma is the cornerstone of the whole formalization effort presented here: all the other results depend on it.

This fact is illustrated in Section 5, where it is informally explained how Lemma 1 can be applied to the particular case of the Vickrey auction.

This informal explanation is then made formal and systematic in Section 6, where ancillary lemmas and definitions are given in order to formally derive from Lemma 1 the main result, Theorem 1, which is the formal statement of our generalized version of NB.

1.2 Notations

- We will represent any function (e.g., the one associating to each participant her bid) in a set-theoretical fashion; that is, as the set $\{(x, f(x)) \,|\, x \in \operatorname{dom} f\}$, commonly called the graph of f. Hence, for example, the cartesian product $X \times \{y\}$ is the constant function defined on X and yielding y.
- Similarly, any relation will be represented as the set of the pairs of elements related through it; formally, this means that any relation is a subset of some cartesian product $X \times Y$.
- Given a relation R, $R(X)$ will be the image of the set X through R: $R(X) := \{y \,|\, (x, y) \in R \text{ and } x \in X\}$. For example, given a function f, $f^{-1}(\{y\})$ will then be the fiber of the point y under f.
- The restriction of a function f to the set-theoretical difference $\operatorname{dom} f \backslash X$ will be written $f - X$; moreover, in the special case of $X = \{x\}$, we will often abuse the notation, writing $f - x$ instead of $f - \{x\}$.
- A multiset (also called a bag) will be extensionally denoted writing, e.g., $\{|0, 0, 1, 1, 1, 2|\}$: we recall that a multiset is similar to a set, but each member has a multiplicity describing how many times it appears in the multiset. We will use $+$ as the infix symbol for pairwise multiset union; we will write $A \leq B$ to express the fact that A is a sub-multiset of B: for instance, $\{|2, 1, 1|\} \leq \{|0, 0, 1, 1, 1, 2|\}$ is true.
- Finally, $x \rightharpoonup X$ denotes the operation of union of x with each set in the family of sets X:

$$x \rightharpoonup X := \{x \cup x' : x' \in X\}.$$

We will need this operation to state Lemma 1.

2   Statement of the main result

An auction mechanism is mathematically represented through a pair of functions a, p: the first describes how the goods at stake are allocated among the bidders (also called participants or agents), while the second specifies how much each bidder pays following this allocation. Each possible output of this pair of functions is referred to as an *outcome* of the auction. Both functions take the same argument, which is another function, commonly called a *bid vector*; it describes how much each bidder prefers each possible outcome of the auction. This preference relation is usually expressed through money, hence the bid vector associates some outcome to how much the participant values that outcome. To stick with traditional notation, we will use bold face for bid vectors, as in $a(\boldsymbol{b})$.

In the case of a single good being auctioned, the bid vector simply associates to each bidder the amount she bids for the good. Given a fixed bidder i, moreover, a_i is $\{0, 1\}$-valued, corresponding to the fact that i either wins the item or not. For a single good auction, the Vickrey mechanism has a special relevance because of the formal properties it enjoys [5, 3]. It works by assigning the good to the highest bidder. Each agent then pays a 'fee' term $p_i'(\boldsymbol{b} - i)$ irrespective of the outcome; this fee does not depend on how much i herself bids, but only on the other participants' bids: hence the argument of p_i' is $\boldsymbol{b} - i$ rather than the full $\boldsymbol{b}$. Additionally, the winner pays a proper price term given by the highest of the bids computed on the set of participants excluding the winner herself (second price); given a fixed bid vector $\boldsymbol{b}$, we will denote this amount as $f_2(\boldsymbol{b})$.

An often desirable property of an auction mechanism is that it achieves *budget balancing* [6, Section 2.3]. This means that the sum of the money given or received by each participant *always* totals to zero:

$$\forall \boldsymbol{b} \qquad\qquad \sum_i p_i(\boldsymbol{b}) = 0. \qquad\qquad (1)$$

Such a property becomes attractive when

> it is preferable to maintain as much wealth as possible within the group of agents, and the transfer payment can be viewed as an undesirable "cost of implementation". [1]

There are important cases in which (1) assumes a more specific form:[‡]

$$\forall \boldsymbol{b} \qquad\qquad \overline{f}(\boldsymbol{b}) + \sum_i p_i'(\boldsymbol{b} - i) = 0, \qquad\qquad (2)$$

where $\overline{f}$ typically extracts some kind of maximum: e.g., for the single-good Vickrey mechanism, $\overline{f}(\boldsymbol{b})$ is the second price $f_2(\boldsymbol{b})$. The function p_i' is related to p_i through a simple construction we are not interested in here. Here, the important fact is the formal difference between p_i and p_i': the former takes as an argument

---

[‡]We recall that bid vectors are modeled as functions, hence we can write $\boldsymbol{b} - i$, using the notation introduced in Section 1.2.

the full bid vector, while the latter takes a *reduced* bid vector, in which the bid pertaining participant i has been removed.

A standard result [6, Theorem 2.2], [5, Proposition 3], [2, Theorem 4.1] is that for such cases, budget balancing cannot be satisfied: (1) is false. Its known proofs, however, all exploit the particular form of the map $\overline{f}$ appearing in (2) in the considered case, namely that of $\overline{f}$ being f_2. Vice versa, we will see a proof starting from (2) where the latter map is considered as an unknown; the proof will work out the conditions it needs to impose on that map: only after that we will ascertain they are fulfilled for the given cases we are interested in (e.g., the mentioned single-good Vickrey auction). To be even more informative, the proof will show that to falsify equation (2), it is not needed to quantify it over all the possible $\boldsymbol{b}$ admissible as an argument to $\overline{f}$: a smaller, finite set X will be suggested by the proof itself.

Hence, we will consider the logical formula

$$\forall \boldsymbol{b} \in X \qquad\qquad \sum_i p'_i\,(\boldsymbol{b} - i) = f\,(\boldsymbol{b}) \qquad\qquad (3)$$

and study for what X and f it leads to a contradiction (which will include, of course, our starting case (2), where $f = -\overline{f}$). Since we are going to set up a proof mechanism minimizing the requirements on the generic f (e.g., we are not going to expect that f is the maximum or the second maximum of the bids), we must impose some different premises to carry through a proof. The main assumption needed is one of symmetry: while the p_is in (1) (and hence the p'_is in (2)) are completely arbitrary, we need to require that they do not depend on re-labeling the participants:

$$\exists P \qquad\qquad \forall i\; \boldsymbol{b} \qquad\qquad p'_i\,(\boldsymbol{b}) = P(\|\boldsymbol{b}\|), \qquad\qquad (4)$$

where $\|R\|$ is the *multiset* (or *bag*) obtained from the relation R: that is, the range of R, but taking into account the multiplicities of possibly repeated values in it.[§] This means that the price paid by any participant i is given by a rule depending only on the amount of each bid other than i's, and not on *who* placed those. Moreover, such a rule itself must not depend on i.

With this assumption in place, (3) becomes

$$\forall \boldsymbol{b} \in X \qquad\qquad \sum_i P\,(\|\boldsymbol{b} - i\|) = f\,(\boldsymbol{b})\,. \qquad\qquad (5)$$

[§]For example, given the map associating to participant 1 the bid 10, to participant 2 the bid 20, and to participant 3 the bid 10, the obtained multiset is $\{|10, 10, 20|\}$.

3 Proof idea

Let N be the number of bidders. The proof starts by considering the case that they all submit the same (fixed but arbitrary) bid b_0, whence (5) yields:

$$P\left(\left\{\left|\underbrace{b_0,\ldots,b_0}_{N-1}\right|\right\}\right) = k_0 f\left(\underbrace{b_0,\ldots,b_0}_{N}\right), \tag{6}$$

with $k_0 := \frac{1}{N}$ not depending on b_0. Then we continue with a $\boldsymbol{b}$ in which only one component (let us say the first, for example) assumes an arbitrary value b_1 different than b_0; thus, (5) gives

$$(N-1)P\left(\left\{\left|b_1,\underbrace{b_0,\ldots,b_0}_{N-2}\right|\right\}\right) = -P\left(\left\{\left|\underbrace{b_0,\ldots,b_0}_{N-1}\right|\right\}\right) - f\left(b_1,b_0,\ldots,b_0\right). \tag{7}$$

At this point, we would like to trigger an iterative mechanism by exploiting (6) inside (7). A natural imposition to make this possible is to ask that

$$f\left(b_1,b_0,\ldots,b_0\right) = q_1 f\left(b_0,\ldots,b_0\right) \tag{8}$$

for some arbitrary constant q_1. Then we can substitute (6) inside (7), obtaining a rational number k_1 not depending on b_0, b_1 such that

$$P\left(\left\{\left|b_1,\underbrace{b_0,\ldots,b_0}_{N-2}\right|\right\}\right) = k_1 f\left(b_0,\ldots,b_0\right). \tag{9}$$

Proceding the same way, we can build a rational constant k_2 such that

$$P\left(\left\{\left|b_1,b_2,\underbrace{b_0,\ldots,b_0}_{N-3}\right|\right\}\right) = k_2 f\left(b_0,\ldots,b_0\right) \tag{10}$$

for arbitrary b_1, b_2.

So that by iterating this mechanism we can construct a relation binding the generic $P\left(\{|b_1,\ldots,b_{N-2},b_0|\}\right)$ to $f\left(b_0,\ldots,b_0\right)$:

$$P\left(\{|b_1,\ldots,b_{N-2},b_0|\}\right) = k_{N-2} f\left(b_0,\ldots,b_0\right). \tag{11}$$

Moreover, at each step of this iteration, the requirement (8) gives indications about how $q_1, q_2, \ldots, X$ and f must be related if we want the proof mechanism to work. It is important to note that, in doing so, such mutual relations should be weakened as much as possible, with the only rationale that they should grant that the proof mechanism just outlined actually works. For example, we imposed

one equality of the kind (8) at each inductive step, but these equalities actually need to hold only for the bid vectors inside some minimal X; otherwise, we would restrict ourselves to quite trivial instances of f. In this section, we wanted to give a general idea of the proof, and we did not explicitly state the exact mutual relations between b_0, X and f. Indeed, such relations are not immediate, at first: they actually became clearer when formalizing the proof itself; a process that we feel would have been harder to manage with a standard paper-based proof. These relations will be given in full detail in Section 4, in Definition 1.

The iteration explained above implies that we assign some value to the numbers $q_1, q_2, \ldots$. We deemed them arbitrary because the proof mechanism works whichever values we assign them. For simplicity, however, we restricted our work to the case

$$1 = q_1 = q_2 = \ldots, \tag{12}$$

which will be general enough for any application to auction theory.

The idea is now to take equation (11), which was obtained using equation (5), and to derive a contradiction between it and (5) itself. Hence, the formalization can be seen as split in two stages: there is Lemma 1, presented in Section 4, which formalizes equation (11) and takes care of spelling out all the exact requirements in order to derive it exploiting the idea we informally presented above. Then there are other auxiliary definitions and lemmas, presented in Section 6, which employ Lemma 1 to obtain the wanted contradiction (given in the thesis of Theorem 1).

4   From the idea to the formal statement

Given a multiset m, an m-restriction of $\boldsymbol{b}$ is any $\boldsymbol{b}' \subseteq \boldsymbol{b}$ such that $\|\boldsymbol{b}'\| = m$.

An m-completion of $\boldsymbol{b}$ to b_0 is a $\boldsymbol{b}'$ writable as the disjoint union of an m-restriction of $\boldsymbol{b}$ with a function constantly valued b_0, and such that $\operatorname{dom} \boldsymbol{b} = \operatorname{dom} \boldsymbol{b}'$. In other words, an m-completion of $\boldsymbol{b}$ to b_0 is obtained from $\boldsymbol{b}$ by changing its value to b_0 outside some m-restriction of it.

A full family of b_0-completions of $\boldsymbol{b}$ is a set containing one m-completion of $\boldsymbol{b}$ to b_0 for each possible $m \leq \|\boldsymbol{b}\|$.

Lemma 1 (`11157`)**.** *Consider a full family Y of b_0-completions of $\boldsymbol{b}$, and set $X := (\{i_1, i_2\} \times \{b_0\}) \rightharpoonup Y$ for some $i_1 \neq i_2$ outside $\operatorname{dom} \boldsymbol{b}$. Assume that, $\forall \boldsymbol{b}' \in X$:*

$$f(\boldsymbol{b}') = f((\{i_1, i_2\} \cup \operatorname{dom} \boldsymbol{b}) \times \{b_0\}) \tag{13}$$

$$f(\boldsymbol{b}') = \sum_{i \in \operatorname{dom} \boldsymbol{b}'} P(\boldsymbol{b}' - i). \tag{14}$$

Then

$$P(\|\boldsymbol{b}\| + \{|b_0|\}) = \frac{1}{2 + |\operatorname{dom} \boldsymbol{b}|} f((\{i_1, i_2\} \cup \operatorname{dom} \boldsymbol{b}) \times \{b_0\}).$$

For later discussion, it will be useful to express requirements in Lemma 1 up to equality (13) in a predicate form:

Definition 1. *[pred2, pred3]*   *The set X is* adequate *for the quintuple $(\boldsymbol{b}, b_0, f, i_1, i_2)$ if*

- *$X = \{i_1, i_2\} \rightharpoonup Y$ for some Y being a full family of b_0-completions of $\boldsymbol{b}$;*
- *$\forall \boldsymbol{b}' \in X \quad f(\boldsymbol{b}') = f((\{i_1, i_2\} \cup \operatorname{dom} \boldsymbol{b}) \times \{b_0\})$.*

This allows us to restate Lemma 1 as

Lemma 2 (`11157`). *Assume that X is adequate for the quintuple $(\boldsymbol{b}, b_0, f, i_1, i_2)$, and that*

$$\forall \boldsymbol{b}' \in X \qquad\qquad \sum_{i \in \operatorname{dom} \boldsymbol{b}'} P(\boldsymbol{b}' - i) = f(\boldsymbol{b}').$$

Then

$$P(\|\boldsymbol{b}\| + \{|b_0|\}) = \frac{1}{2 + |\operatorname{dom} \boldsymbol{b}|} f((\{i_1, i_2\} \cup \operatorname{dom} \boldsymbol{b}) \times \{b_0\}).$$

5   Example application to the Vickrey auction

Let us consider the specific case of $f = -f_2$: we recall that $f_2(\boldsymbol{b})$ is the maximum of the bids $\boldsymbol{b}$, once the bid of the winner has been removed. In this case, choosing any $b_0 \geq \max(\operatorname{rng} \boldsymbol{b})$ satisfies hypothesis (13) of Lemma 1, permitting

$$P(\|\boldsymbol{b}\| + \{|b_0|\}) = \frac{-b_0}{2 + |\operatorname{dom} \boldsymbol{b}|}. \tag{15}$$

Let us apply this to two particular bid vectors:

$$\underline{\boldsymbol{b}} := (1, 2, \ldots, n, n+1, n+3) \qquad \overline{\boldsymbol{b}} := (1, 2, \ldots, n, n+2, n+3).$$

We get

$$f_2(\underline{\boldsymbol{b}}) + \sum_i P(\|\underline{\boldsymbol{b}} - i\|) \overset{(15)}{=} (n+1) - \left[\frac{(n+3)}{n+2}(n+1)\right] - \frac{n+1}{n+2}$$

$$\neq n+2 - \left[\frac{(n+3)}{n+2}(n+1)\right] - \frac{n+2}{n+2} \overset{(15)}{=} f_2(\overline{\boldsymbol{b}}) + \sum_i P(\|\overline{\boldsymbol{b}} - i\|). \tag{16}$$

Thus, we have falsified (2) as an application of Lemma 1. To do that, we had to apply Lemma 1 $n+2$ times for the first equality of the chain above, and further $n+2$ times for its last equality. This corresponds to having imposed (5) on the sets

$$\left\{\{i, j\} \times \{n+3\} \rightharpoonup \mathcal{C}^{n+3}_{\underline{\boldsymbol{b}} - i - j}\right\}_{\substack{\underline{\boldsymbol{b}}(j) = n+3 \\ i \in \operatorname{dom} \underline{\boldsymbol{b}} - \{j\}}} \tag{17}$$

$$\left(\underline{\boldsymbol{b}}^{-1}\{n+1, n+3\}\right) \times \{n+1\} \rightharpoonup \mathcal{C}^{n+1}_{\underline{\boldsymbol{b}} - \underline{\boldsymbol{b}}^{-1}\{n+1, n+3\}} \tag{18}$$

and on the sets

$$\left\{ \{i,j\} \times \{n+3\} \rightharpoonup \mathcal{C}^{n+3}_{\boldsymbol{b}-i-j} \right\}_{\substack{\overline{\boldsymbol{b}}(j)=n+3 \\ i \in \operatorname{dom} \overline{\boldsymbol{b}} - \{j\}}} \tag{19}$$

$$\left(\overline{\boldsymbol{b}}^{-1} \{n+2, n+3\} \right) \times \{n+2\} \rightharpoonup \mathcal{C}^{n+2}_{\boldsymbol{b}-\overline{\boldsymbol{b}}^{-1}\{n+2,n+3\}} \tag{20}$$

respectively. Above, we have indicated with $\mathcal{C}^b_{\boldsymbol{b}}$ a fixed, arbitrary full family of b-completions of $\boldsymbol{b}$. Hence, the union of the family of sets in (17), the union of that in (19), the sets in (18), (20), together with $\left\{ \underline{\boldsymbol{b}}, \overline{\boldsymbol{b}} \right\}$, form the wanted set X: we have a contradiction when imposing (5) on it.

6 Application to the general case

Formally, as a first step of what we did in Section 5, we apply Lemma 1 to each possible $\boldsymbol{b} - i$ appearing in (5), obtaining an equality for the sum featured there. The following result does exactly that and is an immediate corollary of Lemma 2:

Corollary 1 (11168). *Assume that $\forall i \in \operatorname{dom} \boldsymbol{b}$ there are j_i and X_i such that*

$$j_i \in \operatorname{dom} \boldsymbol{b} \backslash \{i\}$$
$$X_i \text{ is adequate for } (\boldsymbol{b} - \{i, j_i\}, \boldsymbol{b}(j_i), f, i, j_i).$$

Also assume that

$$\forall \boldsymbol{b}' \in \bigcup X_i \qquad \sum_{i \in \operatorname{dom} \boldsymbol{b}'} P(\|\boldsymbol{b}' - i\|) = f(\boldsymbol{b}').$$

Then

$$\sum_{i \in \operatorname{dom} \boldsymbol{b}} P(\{|\boldsymbol{b} - i|\}) = \frac{1}{|\operatorname{dom} \boldsymbol{b}|} \sum_{i \in \operatorname{dom} \boldsymbol{b}} f(\operatorname{dom} \boldsymbol{b} \times \{\boldsymbol{b}(j_i)\}). \tag{21}$$

What we informally did in Section 5 was to find $\underline{\boldsymbol{b}}$, $\overline{\boldsymbol{b}}$ to each of which corollary 1 is applicable, but such that the maps $\underline{\eta} : i \mapsto f\left(\operatorname{dom} \underline{\boldsymbol{b}} \times \left\{ \underline{\boldsymbol{b}}\left(\underline{j}_i \right) \right\} \right)$ and $\overline{\eta} : i \mapsto f\left(\operatorname{dom} \overline{\boldsymbol{b}} \times \left\{ \overline{\boldsymbol{b}}\left(\overline{j}_i \right) \right\} \right)$ enjoy the following properties:

1. each assumes exactly two values, call them $\underline{v_1} \neq \underline{v_2}$ and $\overline{v_1} \neq \overline{v_2}$, respectively;
2. of these four values, exactly two are equal, let us say $\underline{v_1} = \overline{v_1}$, while $\underline{v_2} \neq \overline{v_2}$;
3. the sets $\underline{\eta}^{-1}\{\underline{v_1}\}$ and $\overline{\eta}^{-1}\{\underline{v_1}\}$ coincide: that is, the points on which $\underline{\eta}$ and $\overline{\eta}$ yield the same value are exactly the same.

These facts cause the occurrence of the two identical terms which can be cancelled in expression (16): they are put in square brackets there for clarity. This cancellation is fundamental, because it immediately allows to establish the inequality appearing there. Finding such $\underline{\boldsymbol{b}}$ and $\overline{\boldsymbol{b}}$ is particularly easy in the case

of $f = f_2$, but the same mechanism works for a generic f, leading to a similar cancellation between the two sums

$$\sum_{i \in \operatorname{dom} \underline{\boldsymbol{b}}} f \left(\operatorname{dom} \underline{\boldsymbol{b}} \times \left\{ \underline{\boldsymbol{b}} \left(\underline{j}_i \right) \right\} \right)$$

and

$$\sum_{i \in \operatorname{dom} \overline{\boldsymbol{b}}} f \left(\operatorname{dom} \overline{\boldsymbol{b}} \times \left\{ \overline{\boldsymbol{b}} \left(\overline{j}_i \right) \right\} \right) ;$$

each of those sums is yielded by a separate application of corollary 1, in the right hand side of equation (21).

To formalize the requirements (1), (2), (3) appearing in the list above, we introduce the following definition:

Definition 2 (`counterexample`). *The triple* $\left(\underline{\boldsymbol{b}}, \overline{\boldsymbol{b}}, h \right)$ *is a* counterexample *for the map* f *if* $\operatorname{dom} \underline{\boldsymbol{b}} = \operatorname{dom} \overline{\boldsymbol{b}}$ *and there is a map* g *such that*

$$h \colon (\operatorname{dom} \underline{\boldsymbol{b}}) \to \{f, g\}$$
$$\{0\} \subset \left\{ f \left(\overline{\boldsymbol{b}} \right) - f \left(\underline{\boldsymbol{b}} \right), g \left(\overline{\boldsymbol{b}} \right) - g \left(\underline{\boldsymbol{b}} \right) \right\}.$$

This definition is devised exactly to formulate the following lemma, which is an easy arithmetical statement:

Lemma 3 (`lll69`). *Assume that* $\left(\underline{\boldsymbol{b}}, \overline{\boldsymbol{b}}, h \right)$ *is a counterexample for* f, *and that* $2 \leq |\operatorname{dom} \underline{\boldsymbol{b}}| < +\infty$. *Then*

$$f \left(\underline{\boldsymbol{b}} \right) - \frac{1}{|\operatorname{dom} \underline{\boldsymbol{b}}|} \sum \left(h \left(i \right) \right) \left(\underline{\boldsymbol{b}} \right) \neq f \left(\overline{\boldsymbol{b}} \right) - \frac{1}{|\operatorname{dom} \overline{\boldsymbol{b}}|} \sum \left(h \left(i \right) \right) \left(\overline{\boldsymbol{b}} \right).$$

In turn, the lemma above can finally be combined with corollary 1 into the main theorem:

Theorem 1 (`tt01`). *Assume that* $\left(\underline{\boldsymbol{b}}, \overline{\boldsymbol{b}}, h \right)$ *is a counterexample for* f, *with* $2 \leq |\operatorname{dom} \underline{\boldsymbol{b}}| < +\infty$. *Moreover, assume that*
$\forall i \in \operatorname{dom} \underline{\boldsymbol{b}}$ *there are* $\underline{j}_i$, $\underline{X}_i$, $\overline{j}_i$, $\overline{X}_i$ *satisfying*

$$\underline{j}_i \in \operatorname{dom} \underline{\boldsymbol{b}} \backslash \{i\}$$
$$\underline{X}_i \text{ is adequate for } \left(\underline{\boldsymbol{b}} - \left\{ i, \underline{j}_i \right\}, \underline{\boldsymbol{b}} \left(\underline{j}_i \right), f, i, \underline{j}_i \right)$$
$$f \left(\operatorname{dom} \underline{\boldsymbol{b}} \times \left\{ \underline{\boldsymbol{b}} \left(\underline{j}_i \right) \right\} \right) = \left(h \left(i \right) \right) \left(\underline{\boldsymbol{b}} \right)$$
$$\overline{j}_i \in \operatorname{dom} \overline{\boldsymbol{b}} \backslash \{i\}$$
$$\overline{X}_i \text{ is adequate for } \left(\overline{\boldsymbol{b}} - \left\{ i, \overline{j}_i \right\}, \overline{\boldsymbol{b}} \left(\overline{j}_i \right), f, i, \overline{j}_i \right)$$
$$f \left(\operatorname{dom} \overline{\boldsymbol{b}} \times \left\{ \overline{\boldsymbol{b}} \left(\overline{j}_i \right) \right\} \right) = \left(h \left(i \right) \right) \left(\overline{\boldsymbol{b}} \right).$$

Finally, suppose that

$$\forall \boldsymbol{b}' \in \bigcup_{i \in \mathrm{dom}\,\underline{\boldsymbol{b}}} \underline{X}_i \cup \overline{X}_i \qquad \sum_{k \in \mathrm{dom}\,\boldsymbol{b}'} P\left(\|\boldsymbol{b}' - k\|\right) = f\left(\boldsymbol{b}'\right).$$

Then

$$f\left(\underline{\boldsymbol{b}}\right) - \sum_{i \in \mathrm{dom}\,\underline{\boldsymbol{b}}} P\left(\|\underline{\boldsymbol{b}} - i\|\right) \neq f\left(\overline{\boldsymbol{b}}\right) - \sum_{i \in \mathrm{dom}\,\overline{\boldsymbol{b}}} P\left(\|\overline{\boldsymbol{b}} - i\|\right).$$

7   Conclusions

We developed a result characterizing imbalanced auction mechanisms. Both the theorem and the proof are new to the best of our knowledge, and we informally illustrated the idea behind the proof.

On the formal side, the proof has been implemented in the Isabelle/HOL theorem prover, which is especially important in this case, because the confidence added by the formalization is a significant soundness validation for any new result.

Given a rather general class of auction mechanisms, our theorem provides explicit conditions implying the imbalance condition, and in this sense it can also be regarded as a result in reverse game theory. Moreover, our theorem also explicitly constructs a finite set on which the imbalance condition holds: this can be exploited in concrete implementations to computationally check the imbalance condition only over that known, finite set.

The fact that the proof and the result are new also leaves open many avenues for possible generalizations and improvements. For example, assumption (12) was taken for the sake of simplicity, but less immediate assumptions are also possible. Similarly, Definition 2 is merely the simplest one granting that Lemma 3 holds: there are plenty of ways to achieve the same result, which can lead to different final requirements on f appearing in the statement of Theorem 1. Currently, ForMaRE is following these tracks to investigate further developments of possible interest to its application domain, auction theory.

References

[1] Ruggiero Cavallo. "Optimal decision-making with minimal waste: Strategyproof redistribution of VCG payments". In: *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*. ACM. 2006, pp. 882–889.

[2] Jean-Jacques Laffont and Eric Maskin. "A Differential Approach to Dominant Strategy Mechanisms". In: *Econometrica* 48.6 (1980), pp. 1507–1520.

[3] Christoph Lange, Marco B. Caminati, Manfred Kerber, Till Mossakowski, Colin Rowat, Makarius Wenzel, and Wolfgang Windsteiger. "A qualitative comparison of the suitability of four theorem provers for basic auction theory". In: *Intelligent Computer Mathematics: MKM, Calculemus, DML, and Systems and Projects 2013*. Ed. by Jacques Carette, David Aspinall, Christoph Lange, Petr Sojka, and Wolfgang Windsteiger. Lecture Notes in Artifical Intelligence 7961. Springer-Verlag, 2013, pp. 200–215.

[4] Christoph Lange, Colin Rowat, and Manfred Kerber. "The ForMaRE Project – Formal Mathematical Reasoning in Economics". In: *Intelligent Computer Mathematics*. Ed. by Jacques Carette, David Aspinall, Christoph Lange, Petr Sojka, and Wolfgang Windsteiger. LNCS 7961. Springer, 2013, pp. 330–334. arXiv:`1303.4194 [cs.CE]`.

[5] Eric Maskin. "The unity of auction theory: Milgrom's master class". In: *Journal of Economic Literature* 42.4 (2004), pp. 1102–1115. URL: `http://scholar.harvard.edu/files/maskin/files/unity_of_auction_theory.pdf`.

[6] Paul Milgrom. *Putting auction theory to work*. Churchill lectures in economics. Cambridge University Press, 2004.

[7] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*. LNCS 2283. Springer, 2002.