Sybil-Proofness of Generalized Adaptive Clinching and Implications for Blockchain Mechanism Design*

Chengkai Zhang† Yuhao Li‡ Elaine Shi§ Mengqian Zhang¶
Lirong Xia‖ Qishen Han**

Abstract

The adaptive clinching auction of Dobzinski, Lavi, and Nisan (FOCS'08) is a cornerstone of mechanism design with budget-constrained bidders, and it has since inspired a broad range of extensions to substantially richer market settings. Adaptive clinching enjoys compelling guarantees: it is Pareto optimal, and truthful bidding is a dominant strategy whenever budgets cannot be overreported. In many real-world environments, however, identities are cheap to create, making resilience to Sybil attacks an additional requirement. Whether the guarantees of adaptive clinching survive when a bidder can split its budget across fake identities has remained open. We introduce a generalized framework for adaptive clinching and prove that it satisfies Sybil-robust incentive compatibility: a bidder cannot benefit from splitting into any finite number of identities with arbitrary value reports, provided their aggregate reported budget does not exceed the bidder's enforceable true budget. Sybil resilience thus joins the list of ideal properties of adaptive clinching.

Our work is motivated by practical mechanism-design problems in blockchain-based decentralized finance, where two-asset automated market makers (AMMs) are among the most widely used applications. We design a new *AMM adaptive clinching mechanism* that extends classical adaptive clinching in two ways: it supports a two-sided market and protects against two-sided strategies, and it allows the supply function to depend on the auction state. Its one-sided special case is captured by our generalized adaptive clinching framework, and we further extend our proof techniques to show that the full two-sided mechanism simultaneously satisfies Sybil-robust incentive compatibility and a relaxed notion of Pareto optimality. In light of known impossibility results, together with a new impossibility proved in this paper, we argue that these guarantees are essentially the best possible. More broadly, our work reveals new connections between classical algorithmic game theory and modern decentralized blockchains.

*Author order is randomized with the archived entry.

†Rutgers University. zhangchengkai2002@gmail.com.
‡Columbia University and Carnegie Mellon University. yuhaoli@cs.columbia.edu.
§Carnegie Mellon University. elaineshi@cmu.edu.
¶Carnegie Mellon University. mengqianzhang@cmu.edu.
‖Rutgers University. lirong.xia@rutgers.edu.
**Rutgers University. Hnickc2017@gmail.com.

Contents

1 Introduction **3**
- 1.1 Our Results and Contributions . . . 5
- 1.2 Additional Related Work . . . 7

2 Definitions **10**
- 2.1 AMM Reserve and Cost Curves . . . 10
- 2.2 AMM Mechanism . . . 10
- 2.3 Strategy Space and Utility . . . 12
- 2.4 Desired Properties . . . 14

3 Warmup: The One-Sided AMM Clinching Mechanism **16**
- 3.1 The One-Sided Model and Feasibility Requirements . . . 16
- 3.2 State, Chord Target, and Demand . . . 17
- 3.3 Continuous Evolution . . . 18
- 3.4 Fixed-Price Operations and Events . . . 19
- 3.5 Continuation and Termination . . . 20

4 Proofs for the One-Sided AMM Clinching Mechanism **21**
- 4.1 Abstract Target-Based Clinching Mechanism . . . 21
- 4.2 Derived Form of the Continuous Dynamics . . . 24
- 4.3 The AMM Target Specification Is Admissible . . . 25
- 4.4 Single-Run Structure . . . 27
- 4.5 Feasibility and Efficiency . . . 29
- 4.6 Sybil-Robust Incentive Compatibility . . . 31

5 Full Two-Sided AMM Clinching Mechanism **36**
- 5.1 Dominant and Minority Sides . . . 36
- 5.2 Allocation and Settlement . . . 36

6 Proofs for the Two-Sided AMM Clinching Mechanism **37**
- 6.1 Extended Targets, Termination, and Exact Settlement . . . 38
- 6.2 The Initial Fill and the Imbalance . . . 40
- 6.3 The Value of Additional Spot-Price Supply . . . 40
- 6.4 Sybil-Robust Incentive Compatibility Across Directions . . . 43
- 6.5 Weak Pareto Optimality for Eligible Bids . . . 45

7 Impossibility with Budget Overreporting **46**
- 7.1 Normalization and Basic Consequences . . . 47
- 7.2 Two Large-Budget Comparisons . . . 50
- 7.3 The Contradiction . . . 52

A Fixed and Online Supply as Constant Targets **58**
- A.1 Fixed Divisible Supply . . . 58
- A.2 Exogenous Online Supply . . . 62

A.3 Incentives for Fixed and Online Supply 64

1 Introduction

Automated Market Makers (AMMs) are arguably the most widely used application in decentralized finance (DeFi). An AMM is a smart contract that stands ready to trade with anyone: rather than matching buyers against sellers through an order book, it holds an inventory of assets and quotes an exchange rate determined by a publicly known pricing curve. By far the most common deployment is the two-asset AMM, exemplified by Uniswap [Uni].

In a typical two-asset AMM, users trade one of two assets, denoted X and Y, against a smart contract, which we henceforth also refer to as the *pool*. Initially, the state of the pool is denoted by (x_0, y_0), meaning that the pool holds x_0 units of X and y_0 units of Y. The exchange rate for each trade is determined by a predefined pricing curve. For example, the widely adopted constant-product rule requires

$$(x_0 - x)(y_0 + y) = C$$

for some positive constant C. Thus, starting from state (x_0, y_0), a user who contributes y units of Y to the pool receives x units of X. Following the trade, the pool transitions to state $(x_0 - x, y_0 + y)$, preserving the invariant that the product of the reserves remains equal to C.

Widespread incentive attacks. Because the price a user receives depends on the pool state when its trade executes, and that state is moved by every preceding trade in the same block, an AMM is acutely sensitive to who controls the contents and the ordering of a block. A block builder can exploit this directly. Suppose a user submits an order to buy X with Y. Immediately *before* that order, the builder buys X cheaply for itself, driving the price up to the user's declared *slippage tolerance*—the worst price at which it is still willing to trade. The user's order then executes at that price and pushes the price higher still, and the builder sells immediately *after* it. The builder has thus bought low and sold high within a single block, at essentially no risk, since it sees the user's order before committing to either leg. The two legs are known respectively as *front-running* and *back-running*, and the pair as a *sandwich attack*; a substantial body of work [ZQT+21, Par23, KDC22] documents how prevalent and how profitable such attacks are in practice.

Such incentive attacks are commonly referred to as Miner (or Maximum) Extractable Value (MEV), and the harm they do extends well beyond the users who are sandwiched. Because the profit accrues to whoever controls the contents and ordering of a block, MEV fosters opaque off-chain markets in which block builders, traders, and specialized searchers compete to identify and exploit these opportunities, and it rewards most those participants with the best access to order flow and the deepest capital. These forces push the ecosystem steadily toward centralization. Indeed, a recent measurement study by Yang et al. [YNZ25] found that the top two block builders produce more than 85% of Ethereum blocks, severely undermining the decentralized vision of blockchain systems.

A theory on AMM mechanism design. Motivated by these attacks, a line of work [CWS25, LSZ26, SZCL26] has formulated AMM as a mechanism-design problem. In this formulation, the AMM mechanism receives a *batch* of bids (typically all trade

requests contained in one block). It then decides, for every bid, how much of each asset that bid sends and receives. Each bid comes in one of two directions. A *sell-Y* bid specifies a value v and a budget Q, meaning that it wants to buy X using at most Q units of Y, and that it values each unit of X it acquires at v units of Y. A *sell-X* bid is defined symmetrically.

Two structural features distinguish the problem from traditional auctions. First, the market is *two-sided*: a batch may contain both sell-X and sell-Y bids, which can trade with each other as well as with the pool. Second, the mechanism must *exactly settle*: every token paid out is funded either by an opposite-side bid or by the pool, no outside subsidy is used, no token is discarded, and the end state of the pool lands back on the prescribed pricing curve.

Within this formulation, one may ask for a *dream* AMM mechanism, namely one that simultaneously achieves the following two desiderata.

1. **Sybil-robust incentive compatibility.** The mechanism should encourage truthful bidding by an individual trader, and it should moreover be strategy-proof against a block builder who may itself be a trader with intrinsic value and demand. Concretely, a trader or builder can misreport both its value and its budget, and can inject any finite number of fake bids under pseudonymous identities, carrying arbitrary values and budgets. Further, a builder can arbitrarily sequence the bids contained in the batch. We refer to the resulting incentive notion as Sybil-robust incentive compatibility. We stress that Sybil-robustness is critical in blockchain environments since creating arbitrary pseudonyms is essentially free.
2. **Pareto optimality.** The outcome should be Pareto optimal: no incremental trade among a subset of traders can make some of them better off without making any of them worse off, and no trader can improve its own utility by trading further with the pool.

Throughout the paper, we assume that a strategic builder cannot censor other traders' bids, meaning that every submitted bid must be included in the mechanism's input. This matches the usual assumption in classical mechanism design: a strategic participant may manipulate its own reports, or even inject fake bids (Sybil attacks), but cannot suppress the reports submitted by other participants. In practice, this is ensured in blockchain systems when the underlying consensus protocol provides censorship resilience [AER25, foc, GNR25], a guarantee that major blockchain projects such as Ethereum are committed to offering at the consensus layer [foc]. Such an assumption is also unavoidable: it is known that once censorship is admissible, Sybil-robust incentive compatibility is unattainable in AMM mechanism design even without imposing any efficiency requirement [SZCL26].

Impossibility of a dream AMM mechanism. Unfortunately, such a dream AMM mechanism is unattainable. Shi et al. [SZCL26] and Li et al. [LSZ26] show that Pareto optimality and Sybil-robust incentive compatibility are mutually incompatible for exact-settlement AMM mechanisms. Further, this impossibility holds in a very strong sense, even when the strategy space consists only of single-identity valuation misreports, and even if the mechanism additionally has access to unforgeable auxiliary information attached to each bid (e.g., trusted timestamps on transactions determined by a decentralized sequencer [dec, KZGJ20, KDK22, KDL+23, Kur20, ZSC+20]).

1.1 Our Results and Contributions

In this paper we identify two natural relaxations of the dream specification under which feasibility is restored, and we present an AMM adaptive clinching mechanism that attains it. Both relaxations are needed: neither one on its own restores feasibility, as we explain later in this section, after stating our main feasibility result.

1. *No aggregate budget overreporting.* Our first relaxation restricts the strategy space. A trader may still split itself into arbitrarily many pseudonymous identities and report arbitrary values, but the budgets that its identities declare *in its own trading direction* must sum to at most its true budget. No restriction whatsoever is placed on the budgets that it declares in the *opposite* direction: a trader who genuinely wishes to sell Y may inject sell-X identities carrying arbitrary finite budgets.

   This assumption is well motivated, because a declared budget must be backed by escrowed funds, and that escrow cannot be replenished out of a sibling identity's proceeds during the batch. A trader whose identities collectively declare more than it owns would therefore have to fund the excess up front, which by definition it cannot do. In practice a trader is of course escrow-limited on the opposite side as well, but our guarantees do not need this: they hold even against a deviator that can escrow arbitrarily large opposite-direction budgets.

2. *Weak Pareto optimality.* Our second relaxation weakens the efficiency requirement to *weak Pareto optimality for eligible bids*, a notion suggested by Li et al. [LSZ26] and Shi et al. [SZCL26] for overcoming impossibilities pertaining to full Pareto optimality. A bid is *eligible* if it is willing to trade at the pool's initial spot price. We require that, under truthful reporting, (a) no subset of eligible traders can re-trade among themselves, subject to their post-batch holdings, in a way that Pareto improves their joint utilities; and (b) no eligible trader can strictly improve its utility by making an additional trade with the pool *in the direction of its own type*—a trader who came to sell Y may only sell more Y.

   Intuitively, the impossibility results of Li et al. [LSZ26] and Shi et al. [SZCL26] suggest that incentive compatibility is easier to achieve if the mechanism can raise the price as competition for the pool's output intensifies, and close the batch at a marginal price exceeding the values of the traders it has served — provided that the average price each trader actually pays remains below its value. Weak Pareto optimality opens up our design space in this direction, by not counting such reverse-direction trades with the pool as Pareto improvements.

Our main result. Under these two relaxations, we obtain the following.

Theorem 1.1 (Sybil-robust and weakly Pareto optimal AMM)**.** *Assume that a strategic trader cannot overreport its budget in aggregate across the Sybil identities it submits in its own trading direction. Then there exists an AMM mechanism that is individually rational, exactly settles against the pool, and simultaneously satisfies Sybil-robust incentive compatibility and weak Pareto optimality for eligible bids.*

As argued below, both relaxations are necessary to obtain Theorem 1.1, thus the combination of properties we achieve is essentially *best possible*. Moreover, as discussed later in this section, the techniques used to achieve Theorem 1.1 reveal exciting connections to classical algorithmic game theory.

Necessity of both relaxations. Both relaxations are necessary. If one insists on full Pareto optimality, impossibility persists even when aggregate same-direction budget overreporting is prohibited [SZCL26].[1] Conversely, we prove that if aggregate same-direction budget overreporting is permitted, impossibility persists even after relaxing full Pareto optimality to our weak notion, as stated in the following theorem:

Theorem 1.2 (Impossibility when overreporting budget is permitted)**.** *Suppose that traders can arbitrarily misreport their values and budgets. Then, no deterministic AMM mechanism can simultaneously satisfy Sybil-robust incentive compatibility and weak Pareto optimality.*

In fact, this impossibility holds in a very strong sense. Its proof needs only deviations that replace a single sell-Y report with another, and does not rely on Sybil identities or opposite-direction orders. Moreover, this impossibility holds even when the mechanism has access to unforgeable auxiliary information attached to each bid.

Zhang et al. [ZXS+26] prove a similar impossibility. In comparison with our Theorem 1.2, their impossibility holds for a much weaker efficiency notion, but it critically relies on the builder's capabilities to reorder bids within a batch, and it ceases to hold if the underlying consensus can provide trusted timestamps on the submitted bids, e.g., generated by a decentralized sequencer [dec, KZGJ20, KDK22, KDL+23, Kur20, ZSC+20] — indeed, a feasibility result [CWS25] is known in this setting satisfying their weaker efficiency notion.

Connections to classical algorithmic game theory. To obtain Theorem 1.1, we generalize the adaptive clinching auction of Dobzinski, Lavi, and Nisan [DLN08], the classical mechanism for multi-unit auctions with hard budget limits. In the classical setting, a *fixed* divisible supply is offered to budget-constrained bidders by an ascending price clock, and a bidder *clinches* a unit precisely when the residual demand of the other bidders no longer covers the remaining supply.

The challenge in our setting is that an AMM has no fixed, exogenous supply: its pricing curve makes the supply available for trade depend on the mechanism's current state. Our central observation is that adaptive clinching extends to this setting by replacing fixed supply with a *carefully chosen state-dependent target*.

Our work reveals exciting connections between classical algorithmic game theory (AGT) and modern blockchain mechanism design. On one hand, our results give a compelling demonstration of how classical AGT ideas contribute to the formation of a much needed scientific foundation for incentive-compatible blockchain markets. On the other hand, the proof techniques developed for our AMM setting advance the state-of-the-art understanding of classical AGT — in particular, we show that the fixed-supply adaptive clinching auction of Dobzinski, Lavi, and Nisan [DLN08] satisfies Sybil proofness, as stated in the following theorem.

Theorem 1.3 (Sybil-proofness of fixed-supply adaptive clinching)**.** *In the adaptive clinching auction for a fixed divisible supply, truthful participation as a single identity*

[1] More precisely, the proof of Theorem 26 in Shi et al. [SZCL26] uses no deviation that overreports a budget. The only required adjustment is to replace their implication from incentive compatibility to no free lunch with Fact 2.9, which establishes the corresponding implication for our restricted strategy space.

weakly dominates every strategy that replaces the bidder with finitely many identities having arbitrary reported values and aggregate declared budget at most the bidder's true budget.

Theorem 1.3 strengthens the incentive guarantees previously established for adaptive clinching with fixed divisible supply [DLN08, BCMX10]. The previous analyses allow value misreports and, in the case of Bhattacharya et al. [BCMX10], budget under-reporting, but do not prove any guarantees in the presence of pseudonymous splitting.

The fixed-supply auction is not obtained directly as a special case of our AMM mechanism. Instead, our proofs introduce an abstract target-based clinching framework that embodies both mechanisms as special cases. We establish Sybil-robust incentive compatibility at this abstract level, thus extending the guarantees to any auction that falls within this target-based clinching framework. This new framework, which can be viewed as a generalization of the ordinary adaptive clinching, may be of independent interest. For example, to demonstrate its usefulness, we show that the framework also captures the adaptive clinching mechanism with exogenous online supply introduced by Goel, Mirrokni, and Paes Leme [GMP13], yielding the following consequence:

Theorem 1.4 (Sybil-proofness with exogenous online supply)**.** *At every positive-supply step of the adaptive clinching mechanism with an exogenous online supply path, truthful participation as a single identity weakly dominates, in cumulative utility, every strategy that replaces the bidder with finitely many identities having arbitrary reported values and aggregate declared budget at most the bidder's true budget.*

1.2 Additional Related Work

AMM mechanism design. Our study builds directly on the AMM mechanism-design framework introduced by Chan et al. [CWS25]. They also construct a Sybil-robust incentive-compatible mechanism, but their result has two limitations. First, their mechanism does not achieve weak Pareto optimality (wPO). It instead satisfies weak local efficiency (wLE) for eligible users, which corresponds to only the pool-trade clause of our wPO definition. Theorem 1.2 shows that this loss of efficiency is unavoidable in their strategy space, which permits a trader to overreport its aggregate budget. Second, they require an overly stringent assumption, that the consensus layer assigns a trustworthy arrival time to every bid. Although a line of work [dec, KZGJ20, KDK22, KDL+23, Kur20, ZSC+20] has explored how to provide such a trusted timestamp, existing schemes are known to be manipulatable, e.g., by a client who deliberately creates Condorcet cycles [VK23].

Subsequent work [LSZ26, SZCL26] further delineates the feasibility frontier in this model. Li et al. [LSZ26] prove a trilemma among incentive compatibility, weak local efficiency, and uniform pricing: any two of these properties can be achieved, but no mechanism can satisfy all three. Thus, contrary to a common intuition, clearing a batch at a uniform price does not by itself yield strong MEV resilience while preserving even weak local efficiency.

Li et al. [LSZ26] and Shi et al. [SZCL26] also show that full Pareto optimality is fundamentally incompatible with Sybil-robust incentive compatibility. Shi et al. [SZCL26]

circumvent this barrier by relaxing exact settlement to permit "burning". Their model allows the pool to release more units than are allocated to traders, with the surplus diverted for the benefit of the broader community. For example, the surplus can subsidize transaction fees, reward liquidity providers, or be returned to the pool to reduce the price impact of future trades. Under this relaxation, they construct a simple and computationally efficient "dream" AMM that achieves both full Pareto optimality and Sybil-robust incentive compatibility.

Sybil proofness in mechanism design. Sybil-proofness, also known as false-name-proofness, has been studied in a variety of settings, including voting [Con08, ABEP11], resource exchange [CDLY22], and combinatorial auctions [SYM99, YSM01, YSM04, ICO+10]. A recurring theme is that auctions that are truthful when identities cannot be faked may cease to be truthful once Sybil attacks are possible; most notably, the VCG mechanism is not false-name-proof in general [SYM99, YSM04, GLT20]. To the best of our knowledge, the Sybil resilience of adaptive-clinching-style auctions for divisible goods under budget constraints has not been analyzed before. The closest related works are those of Iwasaki et al. [IYT03] and Sakurai et al. [SSIY08]. Both works aim to design Sybil-resilient auctions for indivisible goods. Iwasaki et al. [IYT03] focuses ona setting without budget constraints, and Sakurai et al. [SSIY08] considers non-quasi-linear utilities which include budget constraints. Since their settings and auction mechanics are fundamentally different from ours, their Sybil-proofness arguments do not carry over to our setting. Moreover, both Iwasaki et al. [IYT03] and Sakurai et al. [SSIY08] sacrifice efficiency to obtain Sybil resilience. In fact, in the setting of Iwasaki et al., Pareto efficiency is known to be incompatible with Sybil-proofness [YSM04]. Thus Iwasaki et al. evaluate efficiency only empirically, through simulations, and Sakurai et al. leave the analysis of efficiency loss to future work. In contrast, we identify meaningful relaxations under which we provide provable efficiency guarantees.

Adaptive clinching and extensions. The original work by Dobzinsi et al. [DLN08] that proposed the adaptive clinching auction assumed that the budgets are public (i.e., unforgeable). The subsequent work of Bhattacharya et al. [BCMX10] show that, for a divisible good, underreporting a budget is never profitable, so adaptive clinching is incentive compatible as long as budgets cannot be overreported. It is also known that with private budgets, simultaneously achieving incentive compatibility and Pareto optimality is impossible [DLN08]. Our feasibility and infeasibility pair (Theorem 1.1 and Theorem 1.2) can thus be viewed as AMM analogue of classical budget-constrained auctions of divisible goods.

Adaptive clinching [DLN08] has been extended to polymatroidal environments, including the AdWords polytope for sponsored search with multiple keywords and slots [GMP12], as well as to other sponsored-search and combinatorial settings [CBHLS12, FLSS11], heterogeneous items [DHS12], two-sided markets [HS22], online supply [GMP13], and payment constraints more general than hard budgets [GMP14]. Most of these works assume public budgets, and none considers Sybil identities. More fundamentally, in all of them the feasible allocations are fixed exogenously or, with online supply, revealed independently of the bids. In an AMM, the supply is instead created by the very payments the auction collects, along the pool's cost curve. Our target-based

framework captures this endogenous supply, and it recovers fixed and online supply as constant targets (Appendix A). Our two-sided setting also differs from that of Hirai and Sato [HS22], whose sellers are assumed to be truthful and are paid at least their reserve prices. In contrast, our pool must receive exactly the amount that returns it to its curve, and traders in both directions are strategic.

Even with public budgets, no deterministic mechanism attains the guarantees of adaptive clinching once identical items may be complements [LM12], marginal values decrease [GMP12, CBHLS12], or items are heterogeneous with multi-dimensional valuations [DHS12]. Another line of work replaces Pareto optimality with approximations of liquid welfare: Dobzinski and Paes Leme [DP14] show that adaptive clinching 2-approximates it when budgets are public, and Lu and Xiao [LX15] improve the ratio to $(1+\sqrt{5})/2$ with a different auction. Devanur et al. [DHH13] use clinching as a building block for prior-free revenue and welfare guarantees when agents share a common budget. We instead retain an exact, albeit weaker, Pareto guarantee.

Other related work. Ferreira and Parkes [FP23] suggest having the consensus layer enforce verifiable, application-specific sequencing rules that limit how a block builder may order transactions, and they give such rules for AMMs with weak but provable guarantees against MEV extraction. Their approach has several limitations. First, it places application-specific logic in the consensus layer, a shared infrastructure layer that ought to remain application agnostic. Second, their framework is overly restrictive and requires transactions to be executed one by one in the order in which they appear in the block, thus leading to strong impossibilities. In particular, risk-free profit cannot be eliminated in their model.

Among other work on AMMs, Milionis, Moallemi, and Roughgarden [MMR24] characterize profit-maximizing demand curves for a market maker among those that elicit truthful reports from traders. Since traders in their model trade directly with the market maker, strategic ordering and attacks such as front-running and back-running fall outside its scope. Bartoletti et al. [BCLL22] compute a block builder's optimal MEV-extraction strategy — their goal is to characterize MEV extraction rather than to prevent it.

Batch trading has also been studied as an approach to mitigating MEV. Canidio and Fritsch [CF23, CF24] propose a function-maximizing AMM and analyze the elimination of arbitrage profits under idealized perfect competition among arbitrageurs sharing a common external reference price. CoW Protocol [cow] deploys batch trading through competition among solvers. Canidio and Henneke [CH24] propose fair combinatorial auctions for trade intents, studying the trade-off between execution fairness and total value returned to traders under strategic solver bidding. Ramseyer et al. [RGGM24] study equilibrium computation and design trade-offs for batch exchanges incorporating CFMMs. These works do not establish incentive compatibility for finite populations of strategic traders, which is our focus. Within the AMM mechanism-design framework discussed above, Li et al. [LSZ26] show that uniform pricing cannot be combined with both incentive compatibility and weak local efficiency.

In a smart-contract implementation, the escrow that prevents budget overreporting must be protected against flash loans [QZLG21], which would let a trader borrow funds and repay the loan within the same transaction. The attack can be avoided by splitting execution into two phases: traders escrow their budgets in one block, and the batch is

settled in a later block, so that no flash loan can span both.

2 Definitions

2.1 AMM Reserve and Cost Curves

There are two divisible assets, X and Y. The AMM pool has initial reserves $(x_0, y_0) \in \mathbb{R}^2_{++}$. Its reserve curve is

$$\mathcal{R}_\varphi := \{(x, \varphi(x)) : x > 0\}.$$

During a batch, every pool trade settles on this reserve curve.

Definition 2.1 (Admissible AMM)**.** The AMM is *admissible* if $\varphi : (0, \infty) \to (0, \infty)$ is continuous, strictly decreasing, and convex, satisfies

$$\lim_{x \downarrow 0} \varphi(x) = \infty, \qquad \lim_{x \uparrow \infty} \varphi(x) = 0,$$

and is differentiable at x_0, where $y_0 = \varphi(x_0)$. The *spot price* of one unit of X, measured in units of Y, is

$$p_0 := -\varphi'(x_0) > 0.$$

For a net release $z < x_0$ of asset X, define the signed pool cost

$$C(z) := \varphi(x_0 - z) - y_0.$$

Here $z > 0$ means that the pool releases z units of X, whereas $z < 0$ means that it absorbs $-z$ units. Correspondingly, $C(z)$ is the net amount of Y received by the pool and may be negative. The function C is continuous, strictly increasing, and convex, with

$$C(0) = 0, \qquad \lim_{z \uparrow x_0} C(z) = +\infty, \qquad \lim_{z \to -\infty} C(z) = -y_0, \qquad C'(0) = p_0.$$

Thus sending $y \geq 0$ units of Y into the pool releases $C^{-1}(y) \in [0, x_0)$ units of X, while sending $x \geq 0$ units of X into the pool releases $-C(-x) \in [0, y_0)$ units of Y. These two compensation maps are continuous, strictly increasing, and concave. Their initial marginal exchange rates are $1/p_0$ and p_0, respectively.

Constant product as a special case. If $\varphi(x) = x_0 y_0 / x$, then

$$C(z) = \frac{y_0 z}{x_0 - z}, \qquad C^{-1}(y) = \frac{x_0 y}{y_0 + y}, \qquad -C(-x) = \frac{y_0 x}{x_0 + x}.$$

Consequently $p_0 = y_0/x_0$, the first compensation map has initial derivative $x_0/y_0 = 1/p_0$, and the second has initial derivative $y_0/x_0 = p_0$. Thus constant product satisfies Definition 2.1.

2.2 AMM Mechanism

A physical trader has one of two types, according to the asset it wishes to sell.

Sell-Y orders. A sell-Y trader k has true type

$$(V_k, Q_k) \in \mathbb{R}^2_{\geq 0},$$

where V_k is its value for one unit of X, measured in units of Y, and Q_k is its true Y-budget. A sell-Y identity i reports

$$(v_i, q_i) \in \mathbb{R}^2_{\geq 0},$$

where v_i has the same units as V_k and q_i is its declared Y-budget. An outcome for this identity consists of $S_{Y,i}$ units of Y sold and $R_{X,i}$ units of X received, with

$$0 \leq S_{Y,i} \leq q_i, \qquad R_{X,i} \geq 0. \tag{1}$$

Its surplus evaluated at the report is $v_i R_{X,i} - S_{Y,i}$. A single sell-Y report is truthful when $(v_i, q_i) = (V_k, Q_k)$.

All values in this paper are denominated in units of Y per unit of X. Thus V_k and v_i are reciprocals of a positive reservation value for one unit of Y expressed in units of X. This convention puts both types of values on the same price scale.

Sell-X orders. A sell-X trader k has true type

$$(U_k, R_k) \in \mathbb{R}^2_{\geq 0},$$

where U_k is its reservation value for one unit of X, measured in units of Y, and R_k is its true X-budget. A sell-X identity i reports

$$(u_i, r_i) \in \mathbb{R}^2_{\geq 0}.$$

It sells $S_{X,i}$ units of X and receives $R_{Y,i}$ units of Y, where

$$0 \leq S_{X,i} \leq r_i, \qquad R_{Y,i} \geq 0. \tag{2}$$

Its surplus evaluated at the report is $R_{Y,i} - u_i S_{X,i}$. A single sell-X report is truthful when $(u_i, r_i) = (U_k, R_k)$.

A sell-Y order is *eligible* if $v_i \geq p_0$, and a sell-X order is eligible if $u_i \leq p_0$. Unless stated otherwise, the truthful types under consideration satisfy $V_k \geq p_0$ for sell-Y and $U_k \leq p_0$ for sell-X. At equality with p_0, either direction may be designated as the trader's type because it is indifferent at the spot price.

AMM mechanism. Let $\mathcal{I}_{\mathrm{Y}}$ and $\mathcal{I}_{\mathrm{X}}$ be the finite sets of reported sell-Y and sell-X identities. An *AMM mechanism* maps the reported orders to an outcome

$$\Big((S_{Y,i}, R_{X,i})\Big)_{i \in \mathcal{I}_{\mathrm{Y}}}, \qquad \Big((S_{X,i}, R_{Y,i})\Big)_{i \in \mathcal{I}_{\mathrm{X}}},$$

satisfying (1) and (2). The mechanism may match the two sides internally and trade the residual imbalance with the AMM pool.

For an outcome, define the net flows into the pool by

$$X_{\mathrm{pool}} := \sum_{i \in \mathcal{I}_{\mathrm{Y}}} R_{X,i} - \sum_{i \in \mathcal{I}_{\mathrm{X}}} S_{X,i}, \qquad Y_{\mathrm{pool}} := \sum_{i \in \mathcal{I}_{\mathrm{Y}}} S_{Y,i} - \sum_{i \in \mathcal{I}_{\mathrm{X}}} R_{Y,i}. \tag{3}$$

Positive values mean that the pool releases X and receives Y; negative values describe the reverse trade. Trades matched internally cancel from both expressions.

Definition 2.2 (Exact-settlement feasibility)**.** An outcome is *exact-settlement feasible* if it satisfies the per-identity constraints (1) and (2), and the terminal pool reserves satisfy

$$(x_0 - X_{\text{pool}}, y_0 + Y_{\text{pool}}) \in \mathcal{R}_\varphi.$$

Equivalently, its net pool flows satisfy

$$X_{\text{pool}} < x_0, \qquad Y_{\text{pool}} = C(X_{\text{pool}}).$$

Thus every unit paid to an identity is supplied by an opposite-side identity or by the pool, and every unit delivered by an identity is received by an opposite-side identity or by the pool. The aggregate user flows are exactly the negatives of the pool flows: no outside subsidy is used and no token is discarded. A mechanism is *exact-settlement feasible* if it produces such an outcome for every reported profile.

Definition 2.3 (Individual rationality)**.** A mechanism is *individually rational* if, whenever every physical trader submits its single truthful order, every sell-Y trader k satisfies

$$0 \le S_{Y,k} \le Q_k, \qquad V_k R_{X,k} - S_{Y,k} \ge 0,$$

and every sell-X trader k satisfies

$$0 \le S_{X,k} \le R_k, \qquad R_{Y,k} - U_k S_{X,k} \ge 0.$$

Equivalently, these inequalities say that truthful participation gives every trader finite, nonnegative true utility. A trader that does not trade has utility zero.

Every declared budget is a hard per-identity trading limit. It is escrowed before the batch, cannot be transferred between identities during the batch, and cannot be replenished from another identity's batch proceeds. Transfers and deliveries occur at final settlement.

2.3 Strategy Space and Utility

Strategy space. We consider a strategy space where not only misreporting value and budget is possible, but also the creation of Sybil identities — as long as reports in the same-direction of the trader's true type do not exceed the user's actual budget in aggregate. No cap is imposed on opposite-direction Sybil bids, i.e., the trader's opposite direction budget may be arbitrarily large. The mechanism observes only the reported orders; it does not know which identities are controlled by the same physical trader.

More formally, fix a physical trader k, and let $\mathcal{I}_{\mathrm{Y}}(k) \subseteq \mathcal{I}_{\mathrm{Y}}$ and $\mathcal{I}_{\mathrm{X}}(k) \subseteq \mathcal{I}_{\mathrm{X}}$ denote its sell-Y and sell-X identities.

Definition 2.4 (Admissible two-sided Sybil strategy)**.** An admissible strategy of trader k is a pair of finite collections

$$\big((v_i, q_i)\big)_{i \in \mathcal{I}_{\mathrm{Y}}(k)}, \qquad \big((u_i, r_i)\big)_{i \in \mathcal{I}_{\mathrm{X}}(k)},$$

with nonnegative reports, subject to the following direction-dependent constraint.

1. If k has true sell-Y type (V_k, Q_k), then

$$\sum_{i \in \mathcal{I}_{\mathrm{Y}}(k)} q_i \le Q_k.$$

   The opposite-direction budgets r_i may be arbitrary finite nonnegative numbers.

2. If k has true sell-X type (U_k, R_k), then

$$\sum_{i \in \mathcal{I}_{\mathrm{X}}(k)} r_i \le R_k.$$

   The opposite-direction budgets q_i may be arbitrary finite nonnegative numbers.

The reported values v_i and u_i may also be arbitrary finite nonnegative numbers.

Remark 2.5 (On builder strategies). We may view the builder as a special trader enpowered with one additional strategy: a builder can choose how to sequence the bids within the batch. We omit this sequencing choice from the formal strategy space because our mechanism is *order-insensitive*: it treats the batch as an unordered set of reports, and its rules depend on reported values and budgets but not on positions within the block. Consequently, every ordering of a fixed collection of reports produces the same allocations and payments. Thus, our incentive guarantees (Definition 2.6), based on Definition 2.4, already cover such sequencing strategies.

A builder may have intrinsic value and demand, in which case we may model it as a trader (with sequencing capability); or it may participate solely to seek risk-free profit. Fact 2.9 shows that our incentive notion (Definition 2.6) in fact protects against both types of builders, without requiring a separate builder-specific condition to capture the latter category.

Aggregate net flow and utility. Define trader k's aggregate gross token flows by

$$S_Y(k) := \sum_{i \in \mathcal{I}_{\mathrm{Y}}(k)} S_{Y,i}, \qquad R_X(k) := \sum_{i \in \mathcal{I}_{\mathrm{Y}}(k)} R_{X,i},$$
$$S_X(k) := \sum_{i \in \mathcal{I}_{\mathrm{X}}(k)} S_{X,i}, \qquad R_Y(k) := \sum_{i \in \mathcal{I}_{\mathrm{X}}(k)} R_{Y,i}.$$

Its net changes in token holdings are

$$\Delta_{X,k} := R_X(k) - S_X(k), \qquad \Delta_{Y,k} := R_Y(k) - S_Y(k). \tag{4}$$

Thus $-\Delta_{X,k}$ and $-\Delta_{Y,k}$ are its net sales of X and Y, respectively. Utility is evaluated from these aggregate net flows, not by adding the identities' reported surpluses.

For a true sell-Y type (V_k, Q_k), define

$$\mathrm{Util}_k^{\mathrm{Y}} := \begin{cases} -\infty, & \text{if } -\Delta_{Y,k} > Q_k \text{ or } \big(-\Delta_{Y,k} < 0 \text{ and } \Delta_{X,k} < 0\big), \\ V_k \Delta_{X,k} + \Delta_{Y,k}, & \text{otherwise.} \end{cases} \tag{5}$$

The first catastrophic event means that the trader's net sale of Y exceeds its true budget. The second means that its aggregate trade is strictly opposite to its type: it gains Y while losing X.

For a true sell-X type (U_k, R_k), define

$$\mathrm{Util}_k^{\mathrm{X}} := \begin{cases} -\infty, & \text{if } -\Delta_{X,k} > R_k \text{ or } \big(-\Delta_{X,k} < 0 \text{ and } \Delta_{Y,k} < 0\big), \\ \Delta_{Y,k} + U_k \Delta_{X,k}, & \text{otherwise.} \end{cases} \tag{6}$$

Here the catastrophic events mean that the trader net-sells more X than its true budget, or that it gains X while losing Y.

These utility functions do not penalize a trader merely for receiving a net gain in its budget token when it does not lose the other token. Moreover, the catastrophic budget tests concern net rather than gross sales: receipts through opposite-side identities offset deliveries of the same token.

The truthful merged strategy of a sell-Y type (V_k, Q_k) is the single sell-Y order (V_k, Q_k); its utility reduces to $V_k R_X(k) - S_Y(k)$. The truthful merged strategy of a sell-X type (U_k, R_k) is the single sell-X order (U_k, R_k); its utility reduces to $R_Y(k) - U_k S_X(k)$.

2.4 Desired Properties

Sybil-robust incentive compatibility. Sybil-robust incentive compatibility says that the truthful strategy is profit-maximizing in light of the strategy space defined earlier.

Definition 2.6 (Sybil-robust incentive compatibility)**.** A mechanism is *Sybil-robust incentive compatible* if, for every physical trader, every true type (including ineligible types), every fixed strategy profile of the other traders, and every admissible strategy in Definition 2.4, the true utility from the truthful merged strategy is at least the true utility from the deviation. The applicable utility is (5) for a sell-Y type and (6) for a sell-X type.

Since the strategy space for a block builder — possibly having intrinsic value and demand — is the same as for an ordinary trader, Definition 2.6 simultaneously captures dominant strategy incentive compatibility (DSIC) for individual traders, as well as strategy-proofness for a block builder.

Weak Pareto optimality for eligible bids. Fix a completed, exact-settlement-feasible outcome under truthful reporting. For each eligible user i, define its post-batch holdings and value coefficient by

$$(H_i^X, H_i^Y, t_i) := \begin{cases} (R_{X,i}, Q_i - S_{Y,i}, V_i), & i \text{ is a sell-}Y \text{ user}, \\ (R_i - S_{X,i}, R_{Y,i}, U_i), & i \text{ is a sell-}X \text{ user}. \end{cases} \tag{7}$$

Thus a change $(\delta x_i, \delta y_i)$ in user i's holdings changes its utility by $t_i \delta x_i + \delta y_i$.

Definition 2.7 (Weak Pareto optimality)**.** An exact-settlement-feasible two-sided outcome is *weakly Pareto optimal for eligible bids* if both of the following hold.

1. There is no subset $\mathcal{J}$ of eligible users and no additional internal trade satisfying

$$\sum_{i \in \mathcal{J}} \delta x_i = 0, \qquad \sum_{i \in \mathcal{J}} \delta y_i = 0, \qquad \delta x_i \geq -H_i^X, \qquad \delta y_i \geq -H_i^Y \quad (i \in \mathcal{J})$$

that weakly increases $t_i \delta x_i + \delta y_i$ for every $i \in \mathcal{J}$ and strictly increases it for at least one.

2. No eligible user can make a strictly utility-improving bilateral trade with the pool in the same direction as that user's type, using its post-batch holding of the token it sells. A sell-Y user may tender additional Y to the pool for X, whereas a sell-X user may tender additional X to the pool for Y.

The second condition deliberately excludes a reverse-direction pool trade.

Sybil-robust incentive compatibility implies "no free lunch". In practice, a strategic builder may have no intrinsic value or demand and participate solely to seek a risk-free profit. By risk-free profit, we mean a net gain in one asset without a net loss in the other—that is, a free lunch. We show below that Sybil-robust incentive compatibility (Definition 2.6) rules out such profits, even when the builder may submit identities with arbitrarily large finite budgets in either asset. We begin by formalizing this guarantee as the *no-free-lunch* property.

Definition 2.8 (No free lunch)**.** For any reported profile and any subset of identities $\mathcal{J} \subseteq \mathcal{I}_Y \cup \mathcal{I}_X$, define their aggregate net token gains by

$$\Delta_X(\mathcal{J}) := \sum_{i \in \mathcal{J} \cap \mathcal{I}_Y} R_{X,i} - \sum_{i \in \mathcal{J} \cap \mathcal{I}_X} S_{X,i},$$
$$\Delta_Y(\mathcal{J}) := \sum_{i \in \mathcal{J} \cap \mathcal{I}_X} R_{Y,i} - \sum_{i \in \mathcal{J} \cap \mathcal{I}_Y} S_{Y,i}.$$

A mechanism satisfies *no free lunch* if, for every such profile and subset,

$$\Delta_X(\mathcal{J}) > 0 \implies \Delta_Y(\mathcal{J}) < 0, \qquad \Delta_Y(\mathcal{J}) > 0 \implies \Delta_X(\mathcal{J}) < 0.$$

Thus no subset of identities can gain strictly positively in one token without losing the other token in aggregate.

Fact 2.9 (Sybil-robust IC implies no free lunch)**.** *Every mechanism satisfying Sybil-robust incentive compatibility (Definition 2.6) satisfies no free lunch.*

Proof. Fix a reported profile and a subset $\mathcal{J}$, and abbreviate its net gains as Δ_X, Δ_Y. Keep all reports outside $\mathcal{J}$ fixed. Since the mechanism does not observe ownership, we may interpret $\mathcal{J}$ as the identities of one physical trader. Set

$$Q := \sum_{i \in \mathcal{J} \cap \mathcal{I}_Y} q_i, \qquad R := \sum_{i \in \mathcal{J} \cap \mathcal{I}_X} r_i.$$

By Definition 2.4, submitting these identities is admissible for a sell-Y trader with budget Q, or a sell-X trader with budget R, at any nonnegative true value. Suppose towards a contradiction that $\Delta_X, \Delta_Y \geq 0$, with at least one inequality strict. Neither catastrophic utility condition applies to these net gains.

If $\Delta_Y > 0$, consider a sell-Y trader of true type $(0, Q)$. Its truthful merged utility is $-S_Y^{\mathrm{tr}} \leq 0$, whereas submitting $\mathcal{J}$ gives utility $\Delta_Y > 0$. This contradicts Definition 2.6.

If $\Delta_X > 0$, for each $u \geq 0$ let $s(u)$ and $r(u)$ denote the amounts of X sold and Y received by the single sell-X report (u, R), against the same fixed outside reports. This report is an admissible deviation for a true type $(0, R)$, and its utility for that type is $r(u)$, since $0 \leq s(u) \leq R$. Incentive compatibility for type $(0, R)$ therefore gives

$$r(u) \leq r(0) =: K < \infty \qquad \text{for every } u \geq 0.$$

Choose a finite $U > K/\Delta_X$. The truthful utility of type (U, R) is at most

$$r(U) - Us(U) \le r(U) \le K,$$

whereas its admissible strategy $\mathcal{J}$ gives $\Delta_Y + U\Delta_X > K$. This again contradicts Definition 2.6, proving the claim. □

Shi et al. [SZCL26] also show that their notion of incentive compatibility implies no free lunch, paralleling Fact 2.9. Their result does not apply directly here, however, because their strategy space permits budget overreporting, whereas ours caps a trader's aggregate same-direction reports by its true budget.

3 Warmup: The One-Sided AMM Clinching Mechanism

As a warmup, we first present an AMM clinching mechanism assuming a one-sided market. Specifically, throughout this section, every submitted identity is in the sell-Y direction: it tenders Y and demands X. The full, two-sided mechanism will be introduced later in Section 5.

3.1 The One-Sided Model and Feasibility Requirements

More specficially, we specialize the model of Sections 2.2 and 2.3 to a finite set of sell-Y identities $\mathcal{I}_{\mathrm{Y}}$, with $\mathcal{I}_{\mathrm{X}} = \varnothing$. Thus identity i reports $(v_i, q_i) \in \mathbb{R}^2_{\ge 0}$, where v_i is its value for one unit of X, measured in units of Y, and q_i is its Y-budget. It is eligible exactly when $v_i \ge p_0$; an ineligible identity receives zero. As before, the mechanism observes neither true types nor which identities have a common owner.

Write

$$x_i := R_{X,i}, \qquad y_i := S_{Y,i}.$$

The mechanism chooses $x_i \ge 0$ and $0 \le y_i \le q_i$: identity i receives x_i units of X, sells y_i units of Y, and has reported surplus $v_i x_i - y_i$.

On a truthful profile, identify each physical trader with its unique identity i, write its eligible true type as $(V_i, Q_i) \in [p_0, \infty) \times \mathbb{R}_{\ge 0}$, and set $(v_i, q_i) = (V_i, Q_i)$. Its true utility is then $V_i x_i - y_i$. Indeed, $y_i \le q_i = Q_i$, and the opposite-direction catastrophe in (5) cannot occur because $\Delta_{X,i} = x_i \ge 0$. Same-direction Sybil strategies and their utilities retain the definitions of Definition 2.4 and Section 2.3, specialized to $\mathcal{I}_{\mathrm{X}} = \varnothing$.

On the one-sided domain $0 \le z < x_0$, $C(z)$ is the amount of Y the pool must receive to release z units of X. Define its right marginal ask by

$$a(z) := C'_+(z),$$

so, in particular, $a(0) = p_0$.

For any reported profile, define the aggregate allocation and payment by

$$X := \sum_{i \in \mathcal{I}_{\mathrm{Y}}} x_i, \qquad Y := \sum_{i \in \mathcal{I}_{\mathrm{Y}}} y_i. \tag{8}$$

Because $\mathcal{I}_X = \varnothing$, the two-sided net pool flows (3) specialize to $X_{\text{pool}} = X$ and $Y_{\text{pool}} = Y$. Consequently, Definition 2.2 requires precisely

$$0 \le X < x_0, \qquad Y = C(X). \tag{9}$$

The terminal pool reserves are then

$$(x_0 - X, y_0 + Y) \in \mathcal{R}_\varphi.$$

Likewise, for a truthful one-sided bidder, $S_Y(i) = y_i$ and $R_X(i) = x_i$. The two-sided individual-rationality requirement in Definition 2.3 therefore specializes to

$$0 \le y_i \le Q_i, \qquad V_i x_i - y_i \ge 0.$$

The mechanism below is designed to satisfy these specializations of the two-sided requirements. Allocations and payments are generated by an ascending price clock p, starting at the spot price p_0.

3.2 State, Chord Target, and Demand

At clock price p, identity i has cumulative allocation x_i, cumulative payment y_i, and effective remaining budget b_i. While the identity remains in the auction, $b_i = q_i - y_i$. When it exits without spending all of its budget, the unspent amount is cancelled and b_i is set to zero. Together with the aggregate allocation X and payment Y defined in (8), let

$$B := \sum_{i \in \mathcal{I}_Y} b_i$$

denote the aggregate effective remaining budget.

The mechanism starts from

$$p = p_0, \qquad x_i = y_i = 0, \qquad X = Y = 0. \tag{10}$$

Ineligible reports are removed as specified above. Every remaining identity initially has $b_i = q_i$.

After the target below is computed, all events at p_0 are processed before the clock rises. In particular, if $T^{\text{amm}}(p_0, 0, 0) > 0$, that initial target is released as a supply lump, and identities with $v_i = p_0$ are treated as exiting identities. For the AMM, a positive initial target occurs precisely when C has a nontrivial initial linear piece of slope p_0. Thus the general event order below also covers the initial state.

For any state satisfying $Y \ge C(X)$, define

$$g_p(z) := C(z) - Y - p(z - X), \qquad z \in [X, x_0).$$

The *AMM chord target* is

$$T^{\text{amm}}(p, X, Y) := \max\{z \in [X, x_0) : g_p(z) \le 0\}. \tag{11}$$

The maximum exists: the set is nonempty because $g_p(X) \le 0$, it is an interval by convexity, and it is bounded away from x_0 because $C(z) \to \infty$. At its right endpoint,

$$C(T^{\text{amm}}) = Y + p(T^{\text{amm}} - X), \qquad a(T^{\text{amm}}) \ge p.$$

The residual supply offered to the auction at the current price is

$$S := T^{\mathrm{amm}} - X.$$

Geometrically, T^{amm} is the rightmost intersection of C with the line of slope p through (X, Y). Notice that a purchase of $\delta \le S$ at price p changes the state to

$$X^+ = X + \delta, \qquad Y^+ = Y + p\delta,$$

but leaves $Y - pX$, and hence T^{amm}, unchanged. The purchase reduces residual supply from S to $S - \delta$.

At the current price p, define

$$\mathsf{Active} := \{i : v_i > p,\ b_i > 0\}, \qquad \mathsf{Exit} := \{i : v_i = p,\ b_i > 0\}. \tag{12}$$

Thus Active is the set of active identities and Exit is the set of exiting identities that have not yet been processed. Until an exiting identity is processed, its budget remains part of B. Write

$$D_i := \frac{b_i}{p}, \qquad D_{-i} := \sum_{j \neq i:\, b_j > 0} \frac{b_j}{p}$$

for its demand and the demand of the other unprocessed identities. The mechanism maintains the supply invariant

$$S \le D_{-i} \qquad \text{for every } i \in \mathsf{Active}. \tag{13}$$

The set of clinching identities is

$$\mathsf{Clinch} := \{i \in \mathsf{Active} : S = D_{-i}\}. \tag{14}$$

It is convenient to introduce the water level

$$h := B - pS.$$

Since $pD_{-i} = B - b_i$, the invariant and clinching condition are equivalently

$$b_i \le h \quad \text{for every } i \in \mathsf{Active}, \qquad \mathsf{Clinch} = \{i \in \mathsf{Active} : b_i = h\}. \tag{15}$$

3.3 Continuous Evolution

We use the clock price itself as the time variable, so $\mathrm{d}p/\,\mathrm{d}p = 1$. Consider an open interval containing no valuation exit, no discontinuity of the target, no change in the clinching set, and no terminal event. The clock and state paths are absolutely continuous on such an interval, and the target is always reevaluated from the algebraic identity

$$T^{\mathrm{amm}} = T^{\mathrm{amm}}(p, X, Y), \qquad S = T^{\mathrm{amm}} - X, \qquad h = B - pS. \tag{16}$$

The continuous evolution is defined by the following primitive conditions. An identity outside Clinch does not trade:

$$\frac{\mathrm{d}x_i}{\mathrm{d}p} = \frac{\mathrm{d}y_i}{\mathrm{d}p} = \frac{\mathrm{d}b_i}{\mathrm{d}p} = 0, \qquad i \notin \mathsf{Clinch}. \tag{17}$$

Every identity in Clinch receives a nonnegative allocation at the current price, spends exactly that payment from its effective budget, and remains tight at the water level:

$$\frac{\mathrm{d}x_i}{\mathrm{d}p} \geq 0, \qquad \frac{\mathrm{d}y_i}{\mathrm{d}p} = p\frac{\mathrm{d}x_i}{\mathrm{d}p}, \qquad \frac{\mathrm{d}b_i}{\mathrm{d}p} = -\frac{\mathrm{d}y_i}{\mathrm{d}p}, \qquad \frac{\mathrm{d}}{\mathrm{d}p}(b_i - h) = 0, \quad i \in \mathsf{Clinch}. \tag{18}$$

Equations (16)– (18) form a differential-algebraic definition of the continuous auction path. They say directly that trade is charged at the clock price and that an identity which is just able to clinch remains just able to clinch. They apply without modification when $S = 0$: zero residual supply is a boundary state of the same dynamics, not a separate dynamic regime. No trading-rate formula is assumed. In Section 4.2 we prove that these conditions determine a unique rate almost everywhere and derive its explicit form. Upward target jumps are handled by the event rules below.

3.4 Fixed-Price Operations and Events

For use in every event rule, define

$$\mathrm{Buy}(i, \delta; p), \qquad 0 \leq \delta \leq \min\{S, b_i/p\},$$

by

$$x_i \leftarrow x_i + \delta, \qquad y_i \leftarrow y_i + p\delta, \qquad b_i \leftarrow b_i - p\delta.$$

The aggregate variables X, Y, B are updated accordingly. A fixed-price purchase leaves both T^{amm} and $h = B - p(T^{\mathrm{amm}} - X)$ unchanged.

The continuous dynamics stop whenever one of the following events is reached.

1. *A bidder joins the clinching set.* There is no state jump. Add the identity to Clinch and continue with (16)– (18).

2. *A valuation exit.* The identities in Exit are marked as exiting. If the stopping allocation is executed, simultaneous exits are served by the proportional rule specified below; otherwise, their remaining budgets are cancelled simultaneously.

3. *A supply lump.* A lump is an upward jump $\Delta T^{\mathrm{amm}} > 0$ of the target at a fixed price. Incorporate the entire jump by setting

$$T^{\mathrm{amm}} \leftarrow T^{\mathrm{amm}} + \Delta T^{\mathrm{amm}}, \qquad S \leftarrow S + \Delta T^{\mathrm{amm}}. \tag{19}$$

   For the AMM, such a jump can occur only from a settled state $(X, C(X))$ when C has a linear piece of slope p beginning at X. If $[X, X^*]$ is the remainder of the maximal such piece, then $\Delta T^{\mathrm{amm}} = X^* - X$ and the updated target is $T^{\mathrm{amm}} = X^*$. At a price that is both a lump and an exit, incorporate the entire lump before processing any exiting identity.

After incorporating a possible lump and identifying every exit at p, update Active and Exit. Before cancelling any budget or making any restoration purchase, test

$$\sum_{i \in \mathsf{Active}} \frac{b_i}{p} \leq S. \tag{20}$$

If (20) holds, perform the *stopping allocation*. First give every active identity its full demand by applying $\mathrm{Buy}(i, b_i/p; p)$ for every $i \in \mathsf{Active}$. Let

$$L := S - \sum_{i \in \mathsf{Active}} \frac{b_i}{p}, \qquad B_E := \sum_{i \in \mathsf{Exit}} b_i \tag{21}$$

be the residual quantity and the total exiting budget, both evaluated before these purchases. If $B_E > 0$, give each exiting identity the proportional quantity

$$\delta_i := \frac{b_i}{B_E} \min\left\{L, \frac{B_E}{p}\right\}, \qquad i \in \mathsf{Exit}, \tag{22}$$

at price p. Cancel every unspent exiting budget and end the run. At an ordinary exit the current chord is cleared. At a lump, the run may instead end partway through the linear piece: the unallocated suffix is not released by the pool. The proportional rule makes a simultaneous exit independent of how a physical order is partitioned among equal-valued identities.

Suppose instead that (20) fails. With the entire lump already incorporated, cancel all exiting budgets simultaneously:

$$b_j \leftarrow 0 \qquad \text{for every } j \in \mathsf{Exit}, \tag{23}$$

and update B. Define the post-event water level

$$h^\star := B - pS,$$

where B is evaluated after all cancellations. For each $i \in \mathsf{Active}$ with $b_i > h^\star$, apply exactly once

$$\mathrm{Buy}\left(i, \frac{b_i - h^\star}{p}; p\right). \tag{24}$$

These purchases reduce every affected active budget directly to $h^\star$. Each purchase leaves $B - pS$ unchanged, so all purchases use the same post-event water level and their order is immaterial.

Set $h \leftarrow h^\star$, recompute T^{amm}, S, B, update Active, Exit, and Clinch using (12) and (15), and resume the continuous dynamics. The stopping test need not be repeated: cancelling exiting budgets changes neither active demand nor residual supply, while each fixed-price purchase reduces them by the same amount. This one-shot restoration is equivalent to restoring after the lump and again after each exit, because every intermediate restoration purchase leaves the water level unchanged.

3.5 Continuation and Termination

Unless one of the terminal conditions below holds, raise the clock and follow the continuous evolution of Section 3.3 until the next event. This continuation rule applies for every $S \geq 0$. In particular, clearing the current chord does not by itself terminate the mechanism: if $S = 0$ and an active identity remains, the same primitive equations continue to govern the auction while the target is reevaluated as the clock rises.

The mechanism ends in any of the following circumstances:

1. the stopping allocation (20) is executed;

2. after all fixed-price operations at the current price have been processed, no active identity remains;

3. all effective budgets are exhausted.

Upon termination, cancel every unspent effective budget and make no further allocation or payment. The no-active-identity test is made only after a target lump at the same price and the valuation-exit procedure have been processed, so it does not preempt either operation.

There is no additional terminal condition associated with the AMM capacity x_0. At every finite clock price and finite auction state, the chord target satisfies $T^{\text{amm}} < x_0$, and hence the cumulative allocation satisfies $X \le T^{\text{amm}} < x_0$. Thus neither the target nor the allocation reaches the capacity boundary at a finite state. The equality $S = 0$ only says that the current chord has been cleared; if an active identity remains, raising the clock eventually produces a target strictly above X. Exact settlement, individual rationality, and the incentive properties of this outcome are proved in Section 4.

Observe that the rules above refer to the AMM only through the target T^{amm}, its evolution as the clock rises, and the capacity x_0; the cost curve C and its marginal ask a appear only to explain what those rules mean for the AMM. Section 4 exploits this by proving the guarantees for a general target, and then verifying that T^{amm} qualifies.

4 Proofs for the One-Sided AMM Clinching Mechanism

We now prove that the AMM adaptive clinching mechanism satisfies Sybil-robust incentive compatibility as well as weak Pareto optimality for eligible bids. Before we begin our proof, we first define an abstract target-based clinching mechanism in Section 4.1. This more generalized abstract mechanism allows us to isolate the proof arguments from the particular choice of supply function. Specifically, later in Appendix A, we point out that the classical ordinary adaptive clinching auction [DLN08, BCMX10], and its version with exogenous online supply [GMP13], are the special cases in which the target is constant. Thus, our proofs directly imply that these classical adaptive clinching auctions are sybil-proof too.

After defining the abstract target-based mechanism, we derive the explicit continuous rates implied by its primitive conditions. We then verify the abstract requirements directly for the AMM chord target, and establish the structural lemmas for a single run. We next compare a merged run with a Sybil run to prove the desired incentive compatibility properties.

4.1 Abstract Target-Based Clinching Mechanism

The AMM clinching mechanism is driven by its chord target $T^{\text{amm}}(p, X, Y)$, which determines how much cumulative supply is available at each auction state. We now abstract this role from the geometry of the AMM. The resulting target-based mechanism uses the same clinching rules, but allows a general admissible target function. Choosing T^{amm} as its target recovers the AMM mechanism.

Definition 4.1 (Abstract target-based mechanism)**.** An *abstract target-based mechanism* is a five-tuple

$$\mathfrak{T} := (p_\star, \sigma, T_\sigma, \mathcal{D}_\sigma, \overline{X}_\sigma),$$

whose components have the following meanings.

1. $p_\star > 0$ is the initial clock price.
2. σ is an environment description fixed independently of the submitted bids and common to every bid profile being compared. It contains any non-strategic information that the target rule may consult as the clock advances. If no such information is needed like in the AMM clinching case, $\sigma = \emptyset$ and its subscript may be omitted.
3. T_σ is the cumulative target rule. At a state (p, X, Y), it specifies the cumulative quantity that may be allocated.
4. $\mathcal{D}_\sigma$ is the domain of auction states on which the target rule is defined.
5. $\overline{X}_\sigma \in (0, +\infty]$ is the capacity bound.

Thus T_σ is a map from $\mathcal{D}_\sigma$ into $[0, \overline{X}_\sigma]$; its explicit price argument selects any clock-indexed information contained in σ.

At price p, aggregate allocation X, and aggregate payment Y, set

$$S := T_\sigma(p, X, Y) - X.$$

For an admissible abstract target-based mechanism, $T_\sigma(p, X, Y) \geq X$, so S is the part of the cumulative target not yet allocated. For the AMM application, $p_\star = p_0$, σ is trivial, and $T_\sigma = T^{\text{amm}}$; the full specification is verified in Section 4.3.

Definition 4.2 (Admissible abstract target-based mechanism)**.** An abstract target-based mechanism $\mathfrak{T}$ is *admissible* if the following properties hold.

1. *Feasibility and partition independence.* For every $(p, X, Y) \in \mathcal{D}_\sigma$,

   $$X \leq T_\sigma(p, X, Y) \leq \overline{X}_\sigma,$$

   where the specified capacity $\overline{X}_\sigma$ is common to all bid profiles. The target depends on bidders only through (X, Y), and not on their names or on the partition of an aggregate budget among identities.

2. *Fixed-price invariance.* If $0 \leq \delta \leq S$, then the updated state belongs to the domain and

   $$T_\sigma(p, X + \delta, Y + p\delta) = T_\sigma(p, X, Y). \tag{25}$$

3. *Target decreases with mark-to-market gain.* At a common (p, σ), for any two states in the domain,

   $$pX - Y \leq pX' - Y' \quad \Longrightarrow \quad T_\sigma(p, X, Y) \geq T_\sigma(p, X', Y'). \tag{26}$$

   Thus a state with the smaller aggregate mark-to-market gain has the weakly larger target. Equality of the gains forces equality of the targets.

4. *Clock regularity.* If (X, Y) is held fixed, the map $p \mapsto T_\sigma(p, X, Y)$ is nondecreasing and right-continuous, is locally of bounded variation, and has only upward jumps. Away from those jumps it is locally absolutely continuous; write

$$\lambda_\sigma(p, X, Y) := \frac{\mathrm{d}}{\mathrm{d}r} T_\sigma(r, X, Y)\Big|_{r=p} \geq 0 \tag{27}$$

for its almost-everywhere frozen-state clock rate.

5. *Eventual supply release.* For every $(p, X, Y) \in \mathcal{D}_\sigma$ such that $T_\sigma(p, X, Y) = X < \overline{X}_\sigma$, there is a price $p' > p$ for which

$$(p', X, Y) \in \mathcal{D}_\sigma \qquad \text{and} \qquad T_\sigma(p', X, Y) > X. \tag{28}$$

Thus the target may remain equal to X over a waiting interval, but it cannot remain there forever while X is strictly below the specified capacity.

The domain is also required to contain $(p_\star, 0, 0)$ and to be upward closed in its price coordinate: if $(p, X, Y) \in \mathcal{D}_\sigma$, then $(p', X, Y) \in \mathcal{D}_\sigma$ for every $p' \geq p$. These are requirements on one abstract target-based mechanism; none refers to an execution, a merged run, or a Sybil run. A state with $X = \overline{X}_\sigma < +\infty$ is called *capacity-saturated*. Feasibility then forces $T_\sigma(p, X, Y) = X$ at every such state.

The *target-based clinching mechanism* for an admissible $\mathfrak{T}$ is obtained from the AMM mechanism of Section 3 by replacing its AMM-specific variables as follows:

$$(p_0, T^{\mathrm{amm}}, x_0) \longmapsto (p_\star, T_\sigma, \overline{X}_\sigma). \tag{29}$$

Thus reports are eligible when $v_i \geq p_\star$, residual supply is $S = T_\sigma - X$, and the target is bounded by $\overline{X}_\sigma$. An upward jump of T_σ, whether inherent in its price dependence or encoded by σ, is the supply lump in (19). Every state identity, primitive differential condition, event order, stopping allocation, restoration rule, and continuation rule is otherwise unchanged. The analytical quantity λ_σ in (27) is derived from T_σ and is not an additional component of $\mathfrak{T}$. The substitution therefore changes the source of target supply, not the clinching mechanics.

Convention at capacity saturation. Earlier in our AMM clinching mechanism, we never saturate the capacity, that is, $T^{\mathrm{amm}} < x_0$ at every finite state. However, our generalized target-based mechanism may reach capacity saturation at a finite state, so we must explicitly specify what happens afterward. We adopt the following completion convention: attaining capacity does not itself terminate the execution. The clock and ordinary valuation exits continue under the usual rules. Lemma 4.5 shows that this continuation involves no further trade, so we call it the *zero-trade completion convention*. Allocations and payments are therefore already economically final; the continuation only retains effective budgets until their ordinary valuation exits. This prevents unused budgets from being treated as exhausted merely because the available capacity has been fully allocated.

4.2 Derived Form of the Continuous Dynamics

The preceding construction defines the auction through primitive differential conditions, without postulating a trading-rate formula. We now solve those conditions once for an arbitrary admissible abstract target-based mechanism. The resulting identities are consequences of the mechanism and will be used throughout the proofs below.

Lemma 4.3 (Fixed-price accounting)**.** *Suppose δ units are allocated at price p and charged $p\delta$. Then T_σ and $h = B - pS$ are unchanged, while S and the buyer's effective budget decrease by δ and $p\delta$, respectively.*

Proof. Target invariance is (25). The updates are $X^+ = X + \delta$, $B^+ = B - p\delta$, and $S^+ = T_\sigma - X^+ = S - \delta$. Therefore

$$B^+ - pS^+ = B - p\delta - p(S - \delta) = B - pS = h.$$

□

Lemma 4.4 (Explicit continuous dynamics)**.** *Consider an event-free interval on which the frozen-state target rate λ_σ exists, and write $c = |\mathsf{Clinch}|$. The primitive conditions (16)– (18), after the target substitution (29), uniquely determine the state derivatives almost everywhere. Define the derived rate*

$$\gamma := S + p\lambda_\sigma. \tag{30}$$

Then every identity follows

$$\frac{\mathrm{d}x_i}{\mathrm{d}p} = \begin{cases} \gamma/p, & i \in \mathsf{Clinch}, \\ 0, & i \notin \mathsf{Clinch}, \end{cases} \qquad \frac{\mathrm{d}y_i}{\mathrm{d}p} = \begin{cases} \gamma, & i \in \mathsf{Clinch}, \\ 0, & i \notin \mathsf{Clinch}, \end{cases} \tag{31}$$

$$\frac{\mathrm{d}b_i}{\mathrm{d}p} = \begin{cases} -\gamma, & i \in \mathsf{Clinch}, \\ 0, & i \notin \mathsf{Clinch}. \end{cases} \tag{32}$$

The aggregate variables satisfy

$$\frac{\mathrm{d}h}{\mathrm{d}p} = -\gamma, \qquad \frac{\mathrm{d}T_\sigma}{\mathrm{d}p} = \lambda_\sigma, \qquad \frac{\mathrm{d}S}{\mathrm{d}p} = \lambda_\sigma - \frac{c\gamma}{p}. \tag{33}$$

In particular, h is nonincreasing. If, after all same-price events have been processed, $S = 0$ and there is exactly one active identity i, then i is the sole clincher and

$$\frac{\mathrm{d}x_i}{\mathrm{d}p} = \lambda_\sigma, \qquad \frac{\mathrm{d}y_i}{\mathrm{d}p} = p\lambda_\sigma, \qquad \frac{\mathrm{d}b_i}{\mathrm{d}p} = -p\lambda_\sigma, \qquad \frac{\mathrm{d}S}{\mathrm{d}p} = 0. \tag{34}$$

Thus the sole active identity purchases every continuously appearing target increment at its appearance price.

Proof. First suppose $c > 0$. The tightness condition in (18) requires every clincher's budget to have the same derivative as h. Hence their common payment rate can be written

$$\rho := -\frac{\mathrm{d}h}{\mathrm{d}p} = \frac{\mathrm{d}y_i}{\mathrm{d}p} = -\frac{\mathrm{d}b_i}{\mathrm{d}p}, \qquad i \in \mathsf{Clinch}.$$

Current-price charging then gives

$$\frac{\mathrm{d}B}{\mathrm{d}p} = -c\rho, \qquad \frac{\mathrm{d}X}{\mathrm{d}p} = \frac{c\rho}{p}, \qquad \frac{\mathrm{d}Y}{\mathrm{d}p} = c\rho. \tag{35}$$

The last two derivatives point in the fixed-price direction. By (25), they do not move the target; only the frozen-state clock motion does. Therefore

$$\frac{\mathrm{d}T_\sigma}{\mathrm{d}p} = \lambda_\sigma, \qquad \frac{\mathrm{d}S}{\mathrm{d}p} = \lambda_\sigma - \frac{c\rho}{p}.$$

Differentiating $h = B - pS$ and using (35) yields

$$-\rho = -c\rho - S - p\left(\lambda_\sigma - \frac{c\rho}{p}\right) = -S - p\lambda_\sigma.$$

Consequently $\rho = S + p\lambda_\sigma = \gamma$. Since $S \geq 0$ and $\lambda_\sigma \geq 0$, the resulting allocation rates are nonnegative, as required by the primitive conditions. This proves existence and uniqueness of (31)– (33) when $c > 0$.

If $c = 0$, (17) fixes all individual states. Thus $B' = X' = Y' = 0$, while target evolution gives $T'_\sigma = \lambda_\sigma$. Differentiating $S = T_\sigma - X$ and $h = B - pS$ gives the same aggregate identities with $c = 0$. Finally, when $S = 0$ and exactly one active identity remains, its outside demand is zero, so it is the sole clincher. Setting $c = 1$ and $S = 0$ in the formulas just proved gives (34). □

Lemma 4.5 (Capacity saturation is a zero-trade tail)**.** *Suppose a run reaches a capacity-saturated state. Thereafter its aggregate and individual allocations and payments remain constant. The clock and the ordinary valuation-exit accounting may continue, but no identity makes a further purchase.*

Proof. At saturation, $X = \overline{X}_\sigma$. At every allowed future state, target feasibility gives $X \leq T_\sigma \leq \overline{X}_\sigma = X$. Hence $T_\sigma = X$, $S = 0$, and $\lambda_\sigma = 0$. The derived rate is therefore $\gamma = S + p\lambda_\sigma = 0$, so the continuous dynamics make no trade. There can be no future target lump. At a valuation exit with another active identity remaining, the stopping test fails, the exiting budgets are cancelled, and $h^\star = B$; since every remaining budget is at most B, the restoration rule makes no purchase. When no active identity remains, the run terminates with zero residual supply. Thus no event in the completed tail changes an allocation or payment. □

4.3 The AMM Target Specification Is Admissible

For use in the proof, define the marginal-supply function

$$Z(p) := \sup\{z \in [0, x_0) : a(z) \leq p\}, \qquad p \geq p_0. \tag{36}$$

Thus $Z(p)$ is the amount of pool supply available at a right marginal ask of at most p. If a is strictly increasing and continuous, then $Z(p) = a^{-1}(p)$. The generalized-inverse definition in (36) continues to apply when a has flat segments or jumps, because C is convex but need not be strictly convex or differentiable everywhere.

For the AMM, use the state domain

$$\mathcal{D}^{\mathrm{amm}} := \{(p, X, Y) : p \geq p_0,\ 0 \leq X < x_0,\ Y \geq C(X)\}.$$

The inequality $Y \geq C(X)$ says that the current auction state lies on or above the pool cost curve.

Proposition 4.6 (Admissibility of the AMM target specification)**.** *Let σ^{amm} be the trivial environment description. If the reserve curve satisfies Definition 2.1, then*

$$\mathfrak{T}^{\mathrm{amm}} := (p_0, \sigma^{\mathrm{amm}}, T^{\mathrm{amm}}, \mathcal{D}^{\mathrm{amm}}, x_0)$$

is an admissible abstract target-based mechanism with unattained capacity. Its target-based clinching mechanism is the mechanism of Section 3.

Proof. Fix $(p, X, Y) \in \mathcal{D}^{\mathrm{amm}}$ and write $g_p(z) = C(z) - Y - p(z - X)$. The sublevel set

$$\{z \in [X, x_0) : g_p(z) \leq 0\}$$

contains X, is an interval by convexity, and is bounded away from x_0 because $C(z) \to +\infty$. It therefore has a right endpoint $T^{\mathrm{amm}} \in [X, x_0)$. Continuity gives

$$C(T^{\mathrm{amm}}) = Y + p(T^{\mathrm{amm}} - X). \tag{37}$$

The equality also holds when the target equals X, because $g_p(X) < 0$ would make a right neighborhood of X feasible. The right derivative of g_p at its right endpoint is nonnegative, hence $a(T^{\mathrm{amm}}) \geq p$. This proves target feasibility and the capacity bound. The formula uses no individual reports, proving partition independence.

For a fixed-price purchase $0 \leq \delta \leq T^{\mathrm{amm}} - X$, every candidate $z \geq X + \delta$ satisfies

$$\begin{aligned} C(z) - (Y + p\delta) - p\Big(z - (X + \delta)\Big) \\ = C(z) - Y - p(z - X). \end{aligned}$$

Thus the right endpoint is unchanged. Moreover, convexity and the endpoint inequalities imply $g_p(z) \leq 0$ for every $z \in [X, T^{\mathrm{amm}}]$; consequently the updated state still satisfies $Y + p\delta \geq C(X + \delta)$. This proves fixed-price invariance and preservation of the domain.

To prove that the target decreases with mark-to-market gain, put

$$\psi_p(z) := pz - C(z).$$

The chord condition is $\psi_p(z) \geq pX - Y$, where $pX - Y$ is the aggregate mark-to-market gain. The function ψ_p is concave, reaches its rightmost maximum at $Z(p)$, and is strictly decreasing on $[Z(p), x_0)$. The right endpoint of every nonempty superlevel set lies in that interval. Raising the required mark-to-market gain therefore weakly moves the right endpoint to the left, which is exactly (26).

If the state is held fixed and p rises, then for every $z > X$ the quantity $g_p(z)$ weakly decreases. Hence the chord target is nondecreasing. Convexity gives right-continuity and local bounded variation. On a continuous nondegenerate portion with $S > 0$ and $a(T^{\mathrm{amm}}) > p$, differentiating (37) with (X, Y) fixed gives

$$\lambda^{\mathrm{amm}} = \frac{T^{\mathrm{amm}} - X}{a(T^{\mathrm{amm}}) - p} = \frac{S}{a(T^{\mathrm{amm}}) - p}. \tag{38}$$

The only upward discontinuity can occur from a settled state $(X, C(X))$ when the clock reaches $a(X)$ and C is linear from X to the right. The target then jumps to the right endpoint $Z(p)$ of that linear piece. Indeed, the tangent line of slope $p = a(X)$ agrees with C precisely on the maximal such piece and lies below C afterward. These are exactly the supply lumps specified in (19).

Finally, no state with $X < x_0$ exhausts all future AMM supply: because C is finite at X and diverges only as $z \uparrow x_0$, sufficiently large prices produce a target strictly above X. The capacity x_0 is never attained. For the AMM, substituting (38) into the derived rate (30) gives

$$\gamma = S + p\frac{S}{a(T^{\mathrm{amm}}) - p} = S\frac{a(T^{\mathrm{amm}})}{a(T^{\mathrm{amm}}) - p}.$$

At a settled state with one active identity, the target-increment identity (34) traces the generalized marginal-supply path Z, including its linear-piece jumps. Hence every AMM interpretation stated in Section 3 follows from the uniform substitution (29). □

4.4 Single-Run Structure

The next lemmas concern one execution of the target-based clinching mechanism associated with an admissible abstract target-based mechanism. They are proved before any two executions are coupled.

Lemma 4.7 (Event restoration and stopping)**.** *At an event price, include the entire target jump before evaluating the stopping test. Let B_A and B_E be the total active and exiting budgets at that moment. Then:*

1. *the stopping test is equivalent to $B_E \geq h$;*
2. *if it fails, cancelling all exiting budgets gives $h^\star = h - B_E > 0$, and the one-shot purchases $(b_i - h^\star)_+/p$ are feasible and restore $b_i \leq h^\star$ for every active identity;*
3. *the truth value of the stopping test does not change during the fixed-price purchases; and*
4. *the exit of a clinching identity is a stopping event.*

Proof. At the test, $B = B_A + B_E$, so

$$B_A \leq pS = B - h \quad \Longleftrightarrow \quad B_E \geq h.$$

If the test fails, $B_E < h$. Cancellation changes B, and hence h, by $-B_E$, giving $h^\star = h - B_E > 0$. Reducing every budget above $h^\star$ to $h^\star$ restores the water-level inequalities. The total quantity required is feasible because

$$\sum_i (b_i - h^\star)_+ \leq B_A - h^\star = pS.$$

The inequality is immediate if no budget exceeds $h^\star$; otherwise it follows by subtracting at least one copy of $h^\star$ from a subsum of B_A. By Lemma 4.3, every such purchase leaves $h^\star$ fixed and reduces active demand and residual supply by the same amount, proving the second and third statements. Finally, immediately before exiting, a clincher has

$b_i = h$. A simultaneous target jump can only lower the newly computed h, so the total exiting budget is at least the post-jump water level. The first statement then implies stopping. □

Lemma 4.8 (Allocation structure and clincher persistence)**.** *In a continuing run, the following statements hold.*

1. *The supply invariant is equivalent to*

$$b_i \le h \quad (i \in \mathsf{Active}), \qquad \mathsf{Clinch} = \{i \in \mathsf{Active} : b_i = h\}. \tag{39}$$

2. *An identity that has never clinched has received no allocation and made no payment.*

3. *Once an identity clinches, it remains a clincher until the run ends.*

4. *No positive effective budget is exhausted in a continuing run. Hence every identity with $v_i > p$ and positive reported budget is active, and*

$$b_i = \min\{q_i, h\} \qquad (i \in \mathsf{Active}). \tag{40}$$

Proof. Because $pD_{-i} = B - b_i$, the inequality $S \le D_{-i}$ is exactly $b_i \le B - pS = h$, with equality precisely for a clincher. This proves the first statement.

The mechanism allocates only to a current clincher, to an active identity in a restoration purchase, or as part of a stopping allocation. A restoration buyer finishes with budget equal to the water level and therefore becomes a clincher; a stopping allocation ends the run. When $S = 0$ and one active identity remains, that identity is a clincher because the demand of all other identities is zero. Thus a bidder that has never clinched has not traded in any continuing run, proving the second statement.

Between events, Lemma 4.4 decreases a clincher's budget and h at the same rate. At a nonstopping event, the new level is positive and every active budget above it is reduced to it; in particular, every prior clincher is returned to equality. At an event where a clincher exits, Lemma 4.7 says that the run stops. When $S = 0$ and one active identity remains, the primitive tightness condition likewise preserves equality because that identity holds the entire effective budget. This proves persistence.

On a continuous interval a clincher can reach budget zero only when $h = 0$, at which point every active budget is zero. At a nonstopping event the post-event level is strictly positive. Therefore exhaustion of a positive effective budget ends the run. If an active identity has never clinched, the second statement gives $b_i = q_i \le h$; if it has clinched, persistence gives $b_i = h \le q_i$. This proves (40) and the fourth statement. □

Lemma 4.9 (Exited identities in a continuing run)**.** *If a run continues after price p, every identity j with $v_j \le p$ has $x_j = y_j = 0$, and its entire unspent reported budget was cancelled when it exited.*

Proof. If j had clinched before its exit, persistence would make it a clincher at that exit, which would stop the run by Lemma 4.7. If it first received allocation in the stopping allocation at its exit, the run would again have ended. The allocation-structure statement in Lemma 4.8 therefore gives $x_j = y_j = 0$, and the nonstopping exit rule cancels its full budget. □

Lemma 4.10 (Sole survivor for the AMM target)**.** *If a reachable AMM run continues at a state with $S = 0$ and $p > p_0$, then exactly one identity has positive effective budget. In particular, at most one active identity remains.*

Proof. Since $S = 0$, the definition of the water level gives $h = B$. If some identity clinches, its budget is $b_i = h = B$ by (39), so every other effective budget is zero.

Suppose instead that nobody clinches. Clincher persistence implies that nobody has previously clinched, and the allocation-structure statement then gives $X = Y = 0$. But at this state and any $p > p_0$, the function $C(z) - pz$ has right derivative $p_0 - p < 0$ at zero. It is therefore negative for all sufficiently small $z > 0$, so $T^{\mathrm{amm}}(p, 0, 0) > 0$. This contradicts $S = 0$. Thus a clincher exists and is the unique identity with positive effective budget. A continuing run has at least one such identity, completing the proof. □

4.5 Feasibility and Efficiency

We now specialize the single-run structure to the AMM target. All statements in this subsection concern truthful one-sided sell-Y participation.

Theorem 4.11 (Exact settlement and individual rationality)**.** *Every completed one-sided AMM clinching run is exact-settlement feasible. On a truthful profile it is individually rational: for every identity i,*

$$0 \le y_i \le Q_i, \qquad V_i x_i - y_i \ge 0. \tag{41}$$

Proof. We first prove exact settlement. Consider a stopping allocation and use the notation B_A, B_E, h immediately after a possible lump has been included. If $h \ge 0$, the stopping condition $B_E \ge h$ and the proportional exit rule allocate

$$\frac{B_A}{p} + \frac{B_E - h}{p} = \frac{B - h}{p} = S$$

units, so the final chord is cleared in full. Fixed-price invariance and the chord equality give

$$X_f = T^{\mathrm{amm}}, \qquad Y_f = Y + p(T^{\mathrm{amm}} - X) = C(T^{\mathrm{amm}}) = C(X_f).$$

If $h < 0$, the stopping event must follow a target lump: away from an upward target jump, h starts nonnegative, is continuous and nonincreasing by Lemma 4.4, and reaching zero exhausts all active budgets; a nonstopping exit leaves the positive level described in Lemma 4.7. At a lump, the selected chord is a linear piece of C of slope p. Every active and exiting identity exhausts its budget, leaving the suffix $-h/p$ unallocated, but every purchased prefix still satisfies

$$Y_f = Y + p(X_f - X) = C(X_f).$$

Every other terminal case has $S = 0$. The target equality (37) then gives $Y_f = C(X_f)$. In particular, (34) shows that the one-active boundary path moves directly along the pool curve. Thus every terminal state satisfies (9); all pool output is assigned and all payments enter the pool.

For individual rationality, the mechanism never charges more than the reported budget, so truthful reporting gives $y_i \le q_i = Q_i$. Every increment received while

active is priced below $v_i = V_i$, and every increment received at its exit is priced exactly V_i. Therefore

$$y_i = \int p \, \mathrm{d}x_i \le V_i \int \mathrm{d}x_i = V_i x_i.$$

This includes fixed-price event purchases and Stieltjes jumps. Hence (41) holds. □

For a truthful bidder, let

$$r_i := Q_i - y_i$$

denote its terminal unspent Y-budget, and let $a(X_f) = C'_+(X_f)$ be the terminal right marginal pool ask.

Lemma 4.12 (Terminal certificate)**.** *Every completed truthful one-sided run satisfies:*

1. *if $x_j > 0$ and $V_i > V_j$, then $r_i = 0$; and*
2. *if $r_i > 0$, then $V_i \le a(X_f)$.*

Proof. For the first statement, consider how identity j first receives allocation. If it receives allocation while clinching or in a restoration purchase, it remains a clincher until the run ends. If the run reaches its exit at V_j, that exit stops the run; if the run ends earlier, both i and j are still active. In either case the stopping rule gives identity i its full remaining demand and exhausts its budget. If j first receives allocation in that stopping event, the same conclusion follows directly from the stopping rule. If j receives allocation in the one-active boundary regime, every other effective budget, including that of the higher-valued identity i, is already zero. These cases exhaust the allocation rules and prove item 1.

Let p_f be the terminal clock price. We first note that

$$p_f \le a(X_f). \tag{42}$$

At a fully cleared chord this follows from $a(T^{\mathrm{amm}}) \ge p_f$; at a partial lump it follows because the final point lies on a linear piece of slope p_f. In the one-active boundary regime, the bidder either waits below the next ask or trades at the marginal ask, so the same inequality holds.

If identity i exited, then $V_i \le p_f$, and (42) proves item 2. If it did not exit and $r_i > 0$, suppose for contradiction that $V_i > a(X_f)$. Exact settlement places the state at $(X_f, C(X_f))$. By right continuity of the convex cost, a sufficiently small additional amount of X has average incremental cost strictly below V_i, and i has enough value and positive residual budget to purchase some such amount. The continuation rule would not have terminated at X_f, a contradiction. □

Theorem 4.13 (Weak Pareto optimality in the sell-Y direction)**.** *The truthful one-sided AMM clinching outcome is weakly Pareto optimal for eligible bids in the sense of Definition 2.7.*

Proof. First consider an additional internal trade among eligible users. If every user has $r_i = 0$, nobody holds Y that can be tendered, while every holder values its X positively; a Pareto improvement is impossible. Otherwise set

$$\lambda := \max\{V_i : r_i > 0\}.$$

Item 1 of Lemma 4.12 implies that every user holding positive X has value at least λ, while every user able to tender Y has value at most λ.

Represent a proposed internal trade by changes $(\delta x_i, \delta y_i)_i$ in user holdings. Conservation gives $\sum_i \delta x_i = \sum_i \delta y_i = 0$, and the utility change is $V_i \delta x_i + \delta y_i$. Let $Q = \sum_{\delta x_i > 0} \delta x_i$. A user paying Y must have $r_i > 0$, and weak improvement requires

$$-\delta y_i \le V_i \delta x_i \le \lambda \delta x_i.$$

Thus buyers can pay at most λQ. Every supplier of X has positive initial X-holdings after the mechanism and hence value at least λ; weak improvement requires

$$\delta y_j \ge V_j(-\delta x_j) \ge \lambda(-\delta x_j).$$

Suppliers therefore require at least λQ. Conservation forces equality throughout, so every participant's utility change is zero. No strict Pareto improvement exists.

It remains to consider an additional same-direction pool trade. Exact settlement starts it from $(X_f, C(X_f))$. Buying $\delta > 0$ more units of X costs at least

$$C(X_f + \delta) - C(X_f) \ge a(X_f)\delta.$$

Any bidder able to fund the trade has $r_i > 0$, and therefore $V_i \le a(X_f)$ by item 2 of the terminal certificate. Its utility change is nonpositive. This proves both clauses of the one-sided restriction of Definition 2.7. □

4.6 Sybil-Robust Incentive Compatibility

Fix a physical sell-Y bidder with true type (V, Q), where $V \ge p_\star$. In the *merged run* $\mathcal{M}$, it submits the single report (V, Q). In the *Sybil run* $\mathcal{S}$, it submits a finite set G of sell-Y identities

$$(v_i, q_i)_{i \in G}, \qquad q_G := \sum_{i \in G} q_i \le Q. \tag{43}$$

The set N of outside identities, their reports, and the exogenous target state are identical in the two runs. Every unit allocated to an identity in G has the physical bidder's true value V. Thus the two utilities to be compared are

$$U_G^{\mathcal{M}} = V X_G^{\mathcal{M}} - Y_G^{\mathcal{M}}, \qquad U_G^{\mathcal{S}} = V X_G^{\mathcal{S}} - Y_G^{\mathcal{S}}.$$

Lemma 4.14 (Capping value overreports)**.** *Replacing every Sybil value report v_i by $\min\{v_i, V\}$ weakly increases the physical bidder's true utility.*

Proof. The original and capped executions coincide below price V, because value reports affect the mechanism only when identities exit. Allocations made at price V have zero true marginal surplus, whereas allocations made above V have negative true marginal surplus $V - p$. Capping all overreports simultaneously removes only zero- or negative-surplus trades and cannot remove any positive-surplus trade. □

For any fixed set of identities $\mathcal{I}$, let $X_{\mathcal{I}}(p)$ and $Y_{\mathcal{I}}(p)$ denote its cumulative allocation and payment through clock price p. If a run ends, extend both quantities constantly. Define its mark-to-market gain by

$$\Gamma_{\mathcal{I}}(p) := pX_{\mathcal{I}}(p) - Y_{\mathcal{I}}(p). \tag{44}$$

Lemma 4.15 (Mark-to-market identity)**.** *Under current-price charging,*

$$\Gamma_{\mathcal{I}}(p) = \int_{p_\star}^{p} X_{\mathcal{I}}(s)\ \mathrm{d}s.$$

In particular, $\Gamma_{\mathcal{I}}$ is continuous across fixed-price purchases and is locally absolutely continuous, with derivative $X_{\mathcal{I}}$ almost everywhere. If every identity in $\mathcal{I}$ reports at most V, then its aggregate true utility is $\Gamma_{\mathcal{I}}(V)$.

Proof. Current-price charging gives the Stieltjes identity $Y_{\mathcal{I}}(p) = \int_{[p_\star,p]} s\ \mathrm{d}X_{\mathcal{I}}(s)$. Integration by parts yields

$$pX_{\mathcal{I}}(p) - Y_{\mathcal{I}}(p) = p_\star X_{\mathcal{I}}(p_\star) - Y_{\mathcal{I}}(p_\star) + \int_{p_\star}^{p} X_{\mathcal{I}}(s)\ \mathrm{d}s.$$

Every allocation at the initial price is charged $p_\star$, so the first two terms cancel. A jump of $X_{\mathcal{I}}$ at price p is accompanied by the payment jump $p\,\Delta X_{\mathcal{I}}$, making $\Gamma_{\mathcal{I}}$ continuous. If all reports are at most V, no member of $\mathcal{I}$ buys above V, and evaluating (44) at V gives its true utility. □

For a run $\mathcal{R} \in \{\mathcal{M}, \mathcal{S}\}$, write $B_N^{\mathcal{R}}$ for the outsiders' total effective remaining budget and define

$$W_N^{\mathcal{R}} := X_N^{\mathcal{R}} + \frac{B_N^{\mathcal{R}}}{p}. \tag{45}$$

Thus $W_N^{\mathcal{R}}$ is the outsiders' quantity-denominated wealth in run $\mathcal{R}$: the X they have already received plus the amount of X their remaining effective budget could purchase at the current price. At and after a terminal state, all effective budgets are set to zero for this accounting convention. Put

$$\mathrm{GainGap}_G(p) := \Gamma_G^{\mathcal{M}}(p) - \Gamma_G^{\mathcal{S}}(p), \qquad \mathrm{GainGap}_N(p) := \Gamma_N^{\mathcal{S}}(p) - \Gamma_N^{\mathcal{M}}(p).$$

Thus the group gain gap is oriented as merged minus Sybil, whereas the outsider gain gap is oriented as Sybil minus merged. By Lemma 4.15, $\mathrm{GainGap}_G$ and $\mathrm{GainGap}_N$ are locally absolutely continuous and

$$\mathrm{GainGap}_G' = X_G^{\mathcal{M}} - X_G^{\mathcal{S}}, \qquad \mathrm{GainGap}_N' = X_N^{\mathcal{S}} - X_N^{\mathcal{M}} \quad \text{almost everywhere.}$$

Lemma 4.16 (Group allocation gap)**.** *At every price below V at which the merged run continues,*

$$X_G^{\mathcal{M}} - X_G^{\mathcal{S}} \geq \min\{0,\ W_N^{\mathcal{S}} - W_N^{\mathcal{M}} + T^{\mathcal{M}} - T^{\mathcal{S}}\}. \tag{46}$$

Here a target of a run that has already ended is evaluated at its fixed terminal state and the current common price and environment.

Proof. The merged identity is active with positive budget. Its supply invariant is

$$T^{\mathcal{M}} - X^{\mathcal{M}} \leq \frac{B_N^{\mathcal{M}}}{p},$$

and therefore

$$X_G^{\mathcal{M}} \geq T^{\mathcal{M}} - W_N^{\mathcal{M}}. \tag{47}$$

If the Sybil group has never clinched and its run continues, then $X_G^{\mathcal{S}} = 0$ by Lemma 4.8, so $X_G^{\mathcal{M}} - X_G^{\mathcal{S}} \geq 0$. Otherwise, if the Sybil run continues, some group identity i is currently a clincher. Its clinching equality gives

$$T^{\mathcal{S}} - X^{\mathcal{S}} = D_{-i}^{\mathcal{S}} \geq \frac{B_N^{\mathcal{S}}}{p},$$

so $X_G^{\mathcal{S}} \leq T^{\mathcal{S}} - W_N^{\mathcal{S}}$. If the Sybil run has ended, then $B_N^{\mathcal{S}} = 0$, and target feasibility at its terminal state gives $T^{\mathcal{S}} \geq X^{\mathcal{S}}$, hence the same inequality. Subtracting this upper bound from (47) proves (46) in the latter cases, while the first case gives its zero branch. □

Lemma 4.17 (Outsider accounting)**.** *Fix a price $p < V$ at which the merged run continues, and let*

$$\Phi_p(t) := \sum_{j \in N:\, v_j > p} \min\{q_j, t\}.$$

If the Sybil run also continues, then

$$Y_N^{\mathcal{S}} - Y_N^{\mathcal{M}} = \Phi_p(h^{\mathcal{M}}) - \Phi_p(h^{\mathcal{S}}), \tag{48}$$

$$p\Big(W_N^{\mathcal{S}} - W_N^{\mathcal{M}}\Big) = \mathrm{GainGap}_N, \tag{49}$$

and

$$\beta^{\mathcal{M}} - \beta^{\mathcal{S}} = Q - q_G + d_G^{\mathcal{S}} \geq 0, \qquad \beta := Y + B, \tag{50}$$

where $d_G^{\mathcal{S}}$ is the total Sybil budget cancelled so far, including budgets removed as ineligible at the initial price. If the Sybil run has ended, then

$$Y_N^{\mathcal{S}} \geq Y_N^{\mathcal{M}}, \qquad p\Big(W_N^{\mathcal{S}} - W_N^{\mathcal{M}}\Big) \geq \mathrm{GainGap}_N\,. \tag{51}$$

Proof. Suppose both runs continue. By Lemma 4.9, every outsider with $v_j \leq p$ has paid zero and had its full budget cancelled in both runs. Every outsider with $v_j > p$ is active and, by (40), has budget $\min\{q_j, h\}$. Summing its payment $q_j - \min\{q_j, h\}$ proves (48). Since $\beta = Y + B$ equals the sum of initial budgets minus cancelled budgets, the outsider cancellations agree in the two runs, while the merged identity has no cancellation below V. This proves (50). Finally,

$$pW_N = pX_N + B_N = \Gamma_N + Y_N + B_N = \Gamma_N + \sum_{j \in N:\, v_j > p} q_j$$

in both continuing runs, proving (49).

Now suppose the Sybil run ended at $p_1 \leq p$. Capacity saturation is not a terminal event under the completion convention. Every outsider with $v_j > p_1$ was active at its terminal event and exhausted its budget. An outsider with $v_j \leq p_1$ pays zero in the continuing merged run and a nonnegative amount in the Sybil run. Thus $Y_N^{\mathcal{S}} \geq Y_N^{\mathcal{M}}$. Because terminal effective budgets are set to zero,

$$p\Big(W_N^{\mathcal{S}} - W_N^{\mathcal{M}}\Big) = \mathrm{GainGap}_N + Y_N^{\mathcal{S}} - Y_N^{\mathcal{M}} - B_N^{\mathcal{M}}.$$

The last two terms are nonnegative identity by identity: an outsider active in the merged run has paid its full budget in the ended run, and an outsider already exited from the merged run has zero effective budget and zero payment there. Hence $p(W_N^{\mathcal{S}} - W_N^{\mathcal{M}}) \geq \mathrm{GainGap}_N$. □

Theorem 4.18 (Sybil-proofness for an admissible target-based mechanism)**.** *In any admissible abstract target-based mechanism $\mathfrak{T}$, truthful participation as the merged identity (V, Q) weakly dominates every same-direction Sybil strategy (43):*

$$VX_G^{\mathcal{M}} - Y_G^{\mathcal{M}} \geq VX_G^{\mathcal{S}} - Y_G^{\mathcal{S}}. \tag{52}$$

Proof. By Lemma 4.14, it is enough to consider $v_i \leq V$ for every $i \in G$. Then Lemma 4.15 identifies the two utilities with $\Gamma_G^{\mathcal{M}}(V)$ and $\Gamma_G^{\mathcal{S}}(V)$, so it remains to prove $\mathrm{GainGap}_G(V) \geq 0$.

Let $p_1 \leq V$ be the price at which the merged run ends, taking $p_1 = V$ if it continues up to the merged identity's exit. We first show that, for almost every $p \in [p_\star, p_1)$,

$$\mathrm{GainGap}_G \leq \mathrm{GainGap}_N \implies \mathrm{GainGap}'_G \geq \min\{0, \mathrm{GainGap}_N / p\}, \tag{53}$$
$$\mathrm{GainGap}_G \geq \mathrm{GainGap}_N \implies \mathrm{GainGap}'_N \geq \mathrm{GainGap}_N / p. \tag{54}$$

The total mark-to-market gain difference is

$$\mathrm{GainGap}_G - \mathrm{GainGap}_N = (pX^{\mathcal{M}} - Y^{\mathcal{M}}) - (pX^{\mathcal{S}} - Y^{\mathcal{S}}). \tag{55}$$

If $\mathrm{GainGap}_G \leq \mathrm{GainGap}_N$, the fact that the target decreases with mark-to-market gain gives $T^{\mathcal{M}} \geq T^{\mathcal{S}}$. By Lemma 4.17, $W_N^{\mathcal{S}} - W_N^{\mathcal{M}} \geq \mathrm{GainGap}_N / p$, whether the Sybil run continues or has already ended. The group allocation bound then gives

$$\mathrm{GainGap}'_G = X_G^{\mathcal{M}} - X_G^{\mathcal{S}} \geq \min\{0, W_N^{\mathcal{S}} - W_N^{\mathcal{M}} + T^{\mathcal{M}} - T^{\mathcal{S}}\} \geq \min\{0, \mathrm{GainGap}_N / p\},$$

proving (53).

Suppose $\mathrm{GainGap}_G \geq \mathrm{GainGap}_N$. Then the fact that the target decreases with mark-to-market gain gives $T^{\mathcal{M}} \leq T^{\mathcal{S}}$. If the Sybil run has ended, (51) and

$$p \cdot \mathrm{GainGap}'_N = p(X_N^{\mathcal{S}} - X_N^{\mathcal{M}}) = \mathrm{GainGap}_N + Y_N^{\mathcal{S}} - Y_N^{\mathcal{M}} \tag{56}$$

gives (54). If both runs continue, use

$$h = \beta + (pX - Y) - pT_\sigma.$$

Together with (50), (55), and $T^{\mathcal{M}} \leq T^{\mathcal{S}}$, this gives

$$h^{\mathcal{M}} - h^{\mathcal{S}} = (\beta^{\mathcal{M}} - \beta^{\mathcal{S}}) + (\mathrm{GainGap}_G - \mathrm{GainGap}_N) - p(T^{\mathcal{M}} - T^{\mathcal{S}}) \geq 0.$$

The function Φ_p is nondecreasing, so (48) gives $Y_N^{\mathcal{S}} \geq Y_N^{\mathcal{M}}$. Equation (56) again proves (54).

We next show that both gain gaps are nonnegative on $[p_\star, p_1]$:

$$\mathrm{GainGap}_G \geq 0, \qquad \mathrm{GainGap}_N \geq 0.$$

Let

$$\mu := \min\{\mathrm{GainGap}_G, \mathrm{GainGap}_N\}.$$

It is locally absolutely continuous and $\mu(p_\star) = 0$. At almost every price where the relevant functions are differentiable, if $\mu < 0$, then

$$\mu' \geq \frac{\mu}{p}.$$

Indeed, if $\mathrm{GainGap}_G \le \mathrm{GainGap}_N$, then (53) gives

$$\mathrm{GainGap}'_G \ge \min\{0, \mathrm{GainGap}_N/p\} \ge \mu/p.$$

If instead $\mathrm{GainGap}_N \le \mathrm{GainGap}_G$, then (54) gives

$$\mathrm{GainGap}'_N \ge \mathrm{GainGap}_N/p = \mu/p.$$

At equality points the same conclusion follows from the almost-everywhere derivative of the minimum. If μ ever became negative, take the last preceding price p_2 at which $\mu(p_2) = 0$. On the subsequent negative interval,

$$\left(\frac{\mu(p)}{p}\right)' = \frac{p\mu'(p) - \mu(p)}{p^2} \ge 0,$$

which contradicts $\mu(p_2)/p_2 = 0$. Thus $\mathrm{GainGap}_G, \mathrm{GainGap}_N \ge 0$ through p_1.

If $p_1 = V$, this already gives the result. Suppose $p_1 < V$. Capacity saturation is followed by zero-trade completion rather than termination, so the merged run has ended through one of the ordinary terminal rules. Its identity is still below its value and hence has not exited: a stopping allocation gives it its full remaining demand, while either of the other terminal rules is compatible with it remaining active only if its effective budget is zero. Because none of its budget is cancelled below V, it has therefore exhausted its budget: $Y_G^{\mathcal{M}} = Q$. At p_1, let $b_G^{\mathcal{S}}$ and $d_G^{\mathcal{S}}$ be the Sybil group's remaining and cancelled budgets. Since $Y_G^{\mathcal{S}} = q_G - d_G^{\mathcal{S}} - b_G^{\mathcal{S}}$,

$$p_1\Big(X_G^{\mathcal{M}}(p_1) - X_G^{\mathcal{S}}(p_1)\Big) - b_G^{\mathcal{S}} = \mathrm{GainGap}_G(p_1) + Q - q_G + d_G^{\mathcal{S}} \ge 0.$$

Every unit subsequently obtained by the Sybil group costs at least p_1, so its additional allocation is at most

$$\frac{b_G^{\mathcal{S}}}{p_1} \le X_G^{\mathcal{M}}(p_1) - X_G^{\mathcal{S}}(p_1).$$

Consequently $X_G^{\mathcal{M}}(p) - X_G^{\mathcal{S}}(p) \ge 0$ for every $p \in [p_1, V]$. Because $\mathrm{GainGap}'_G = X_G^{\mathcal{M}} - X_G^{\mathcal{S}}$ almost everywhere, $\mathrm{GainGap}_G$ is nondecreasing on that interval. Therefore $\mathrm{GainGap}_G(V) \ge \mathrm{GainGap}_G(p_1) \ge 0$, proving (52). □

Theorem 4.19 (One-sided AMM incentive compatibility)**.** *Fix all reports of the other sell-Y traders. A physical sell-Y trader of true type (V, Q) cannot improve its utility by replacing its truthful merged identity (V, Q) with finitely many sell-Y identities having arbitrary value reports and aggregate reported budget at most Q. Thus the one-sided AMM clinching mechanism is Sybil-robust incentive compatible.*

Proof. By Proposition 4.6, $\mathfrak{T}^{\mathrm{amm}}$ is an admissible abstract target-based mechanism. Apply Theorem 4.18. Since the aggregate Sybil payment is at most the aggregate reported budget, which is at most Q, both sides of (52) are finite utilities under (5) restricted to sell-Y identities. □

Combining Theorems 4.11, 4.13 and 4.19, the one-sided AMM clinching mechanism is exact-settlement feasible, individually rational, weakly Pareto optimal for eligible bids, and Sybil-robust incentive compatible.

5 Full Two-Sided AMM Clinching Mechanism

We now extend our one-sided mechanism in Section 3 to allow both sell-Y and sell-X bids. Types, eligibility, outcomes, and settlement retain their definitions from Section 2.

The idea is to fill the minority side in full at the spot price. Its orders then supply an initial quantity to the other side, which competes for this quantity and additional pool output through the one-sided clinching mechanism. The main additional proof challenge is the treatment of cross-directional strategies, that is, a sell-Y-type user can potentially post sell-X-type bids under its Sybil identities.

5.1 Dominant and Minority Sides

Let $\mathcal{E}_{\mathrm{Y}} \subseteq \mathcal{I}_{\mathrm{Y}}$ and $\mathcal{E}_{\mathrm{X}} \subseteq \mathcal{I}_{\mathrm{X}}$ be the eligible identities. Measure both sides at the spot price in units of X:

$$D_Y := \sum_{i \in \mathcal{E}_{\mathrm{Y}}} \frac{q_i}{p_0}, \qquad D_X := \sum_{i \in \mathcal{E}_{\mathrm{X}}} r_i, \qquad M := \min\{D_Y, D_X\}.$$

The side with the smaller quantity is the *minority*; the other is the *dominant side*. Here M is the minority fill in units of X. If the quantities are equal, designate sell-X as the minority. As shown below, either designation gives full internal matching at p_0 and leaves the pool unchanged.

5.2 Allocation and Settlement

No matter whether sell-Y or sell-X is dominant, ineligible identities receive zero outcomes. The eligible identities are processed as follows — note that minority-fill proceeds are transferred only at final settlement and cannot finance another order in the same batch.

Sell-Y is dominant. Suppose $D_Y \geq D_X$, so sell-X is the minority and $M = D_X$. Fold the minority supply directly into the cost faced by the dominant sell-Y auction:

$$\widetilde{C}_M(z) := \begin{cases} p_0 z, & 0 \leq z \leq M, \\ p_0 M + C(z - M), & M \leq z < M + x_0. \end{cases} \tag{57}$$

The first M units cost p_0 each and represent the sell-X minority orders, whose total compensation is $p_0 M$. After those units are allocated, the cost of further output is the original pool cost. Thus the dominant auction treats internally matched supply and pool supply as a single cost curve. This curve records aggregate supply costs; individual dominant trades are still charged at the auction clock price.

For a state with $Y \geq \widetilde{C}_M(X)$, define its chord target by the same construction as (11):

$$\widetilde{T}_M(p, X, Y) := \max\{z \in [X, M + x_0) : \widetilde{C}_M(z) \leq Y + p(z - X)\}.$$

In particular, even if the original pool cost is strictly convex, the extended cost has a linear segment whenever $M > 0$. This is why the one-sided construction includes supply lumps and does not assume strict convexity. Execute the following rules.

1. Assign each eligible minority identity its full spot-price trade:

$$S_{X,i} = r_i, \qquad R_{Y,i} = p_0 r_i \quad (i \in \mathcal{E}_{\mathrm{X}}).$$

2. Run the one-sided mechanism of Section 3 on the reports $(v_i, q_i)_{i\in\mathcal{E}_{\mathrm{Y}}}$, replacing $(C, T^{\mathrm{amm}}, x_0)$ by $(\widetilde{C}_M, \widetilde{T}_M, M + x_0)$. The clock still starts at p_0. Use the same continuous dynamics, initial lump, event order, proportional exit rule, and continuation rule. If its output is (x_i, y_i), set

$$R_{X,i} = x_i, \qquad S_{Y,i} = y_i, \qquad X_f := \sum_{i\in\mathcal{E}_{\mathrm{Y}}} x_i, \qquad Y_f := \sum_{i\in\mathcal{E}_{\mathrm{Y}}} y_i.$$

3. Settle all transfers simultaneously. The pool releases $X_f - M$ units of X and receives $Y_f - p_0 M$ units of Y.

In Theorem 6.3 we prove that $X_f \geq M$ and $Y_f - p_0 M = C(X_f - M)$, so all these transfers are funded and the net pool trade lies on the original reserve curve.

Sell-X is dominant. Suppose $D_Y < D_X$, so sell-Y is the minority and $M = D_Y$. Exchange the roles of the assets. In the exchanged coordinates the reserve curve is φ^{-1}, the initial spot price is $1/p_0$, and the one-sided pool cost is

$$C^{\mathrm{rev}}(w) := -C^{-1}(-w), \qquad 0 \leq w < y_0.$$

The extended cost, now measured as units of X needed to release w units of Y, is

$$\widetilde{C}_M^{\mathrm{rev}}(w) := \begin{cases} w/p_0, & 0 \leq w \leq p_0 M, \\ M + C^{\mathrm{rev}}(w - p_0 M), & p_0 M \leq w < p_0 M + y_0. \end{cases}$$

At a reverse-auction state, let p^{rev} be the price in units of X per unit of Y, let X^{rev} be the cumulative amount of Y allocated, and let Y^{rev} be the cumulative amount of X paid. Define

$$\widetilde{T}_M^{\mathrm{rev}}(p^{\mathrm{rev}}, X^{\mathrm{rev}}, Y^{\mathrm{rev}}) := \max\{w \in [X^{\mathrm{rev}}, p_0 M + y_0) : \widetilde{C}_M^{\mathrm{rev}}(w) \leq Y^{\mathrm{rev}} + p^{\mathrm{rev}}(w - X^{\mathrm{rev}})\}.$$

Assign each eligible minority sell-Y identity its full spot-price trade: it pays q_i and receives q_i/p_0. Run the one-sided mechanism on the dominant sell-X identities with reported values[2] $1/u_i$, budgets r_i, and clock p^{rev} starting at $1/p_0$, replacing the cost, target, and capacity by $(\widetilde{C}_M^{\mathrm{rev}}, \widetilde{T}_M^{\mathrm{rev}}, p_0 M + y_0)$. An allocation x_i^{rev} and payment y_i^{rev} in this auction mean $R_{Y,i} = x_i^{\mathrm{rev}}$ and $S_{X,i} = y_i^{\mathrm{rev}}$.

6 Proofs for the Two-Sided AMM Clinching Mechanism

We first justify the extended auction and settlement. For incentives, the one-sided Sybil theorem already handles splitting and value reports while the fill is fixed. The

[2]For a report $u_i = 0$, interpret $1/u_i = +\infty$: that identity never exits because of its value. Equivalently, replace $+\infty$ by any finite value larger than the maximum price the reverse clock can reach; Lemma Lemma 6.2 shows that this does not change the outcome.

additional issue is that opposite-direction orders can enlarge that fill or change which side is dominant. A bound on the value of extra spot-price supply handles the former; the initial water level handles the latter. We then use the one-sided terminal certificate to prove weak Pareto optimality for eligible bids from both sides.

6.1 Extended Targets, Termination, and Exact Settlement

Once the minority fill is folded into the dominant side's cost curve, that curve and its domain fully determine the resulting one-sided AMM clinching auction. The curve's right derivative at zero gives the initial clock price, the endpoint of its domain gives the capacity, the condition that an auction state lies on or above the curve gives the state domain, and the chord construction gives the target. Thus the one-sided clinching auction when sell-Y is dominant is determined by $\widetilde{C}_M$, while the reverse auction when sell-X is dominant is determined by $\widetilde{C}_M^{\mathrm{rev}}$.

Lemma 6.1 (The extended auction inherits the one-sided results)**.** *For every fixed $M \geq 0$, the one-sided AMM clinching auction generated by $\widetilde{C}_M$ is an admissible target-based mechanism with unattained capacity $M + x_0$. Its cost curve is continuous, strictly increasing, and convex on $[0, M + x_0)$, starts at zero with right derivative p_0, and diverges at $M + x_0$. The reverse one-sided AMM clinching auction generated by $\widetilde{C}_M^{\mathrm{rev}}$ is likewise admissible; its cost curve has the corresponding properties on $[0, p_0 M + y_0)$, with initial right derivative $1/p_0$ and unattained capacity $p_0 M + y_0$.*

Consequently, the single-run structural lemmas, exact-settlement theorem, and terminal certificate from Section 4 apply to the one-sided auction generated by $\widetilde{C}_M$ and, separately, to the reverse one-sided auction generated by $\widetilde{C}_M^{\mathrm{rev}}$. Same-direction Sybil-robust incentive compatibility (Theorem 4.18) also applies separately to these two auctions.

Proof. The two branches of (57) agree at M, and their slopes meet at $p_0 = C'_+(0)$. The right derivative is p_0 on $[0, M)$ and $a(z - M)$ on $[M, M + x_0)$; it is positive and nondecreasing. The other asserted cost properties follow directly from those of C. The proof of Proposition 4.6 uses precisely these properties of the cost, so it applies with C replaced by $\widetilde{C}_M$. The structural lemmas and Theorem 4.18 then apply to the resulting admissible target. Likewise, the proofs of Theorem 4.11 and Lemma 4.12 use only this chord construction and the same cost properties.

The inverse of a strictly decreasing convex reserve curve is again strictly decreasing and convex. It has the same reserve-limit properties and is differentiable at y_0, with derivative $-1/p_0$. Hence exchanging the assets gives an admissible AMM, and the argument applies to $\widetilde{C}_M^{\mathrm{rev}}$ as well. □

Lemma 6.2 below addresses a boundary case in the reverse auction. When sell-X is dominant, a sell-X report with reservation value $u_i = 0$ has transformed one-sided value $1/u_i = +\infty$. Since our earlier analysis of the one-sided case allows only finite-value reports, it is convenient to replace this infinite transformed value by a sufficiently large finite one without affecting the outcome.

Lemma 6.2 (Infinite bids admit finite truncation)**.** *Let $\widehat{C}$ be either extended cost, let $p_\star$ be its initial clock price, and let B_0 be the total initial budget in that auction. Set*

$$z_B := \widehat{C}^{-1}(B_0), \qquad P_B := \widehat{C}'_+(z_B) < \infty.$$

The run terminates at a finite clock price. Any value report above P_B can be replaced by any other value above P_B, or by $+\infty$, without changing the outcome. In particular, an identity with infinite clock value spends its entire budget.

Proof. At a continuing state after all events at the current price, the structural lemmas give $h > 0$. With $\beta := Y + B \le B_0$, the chord identity gives

$$\widehat{C}(T) = Y + p(T - X) = \beta - h \le B_0, \qquad p \le \widehat{C}'_+(T) \le \widehat{C}'_+(z_B) = P_B.$$

Here z_B lies below the capacity and its right derivative is finite, including when $B_0 = z_B = 0$. Choose a finite $H > P_B$ for every infinite report. With these finite reports the usual termination rule stops the run no later than its largest value report; the bound above forces termination before H. Indeed, a continuing clock could not pass through the interval (P_B, H). Reports above P_B therefore never exit before termination, and their exact values do not affect any allocation rule. This both defines and proves termination for the infinite-report convention. Such an identity is still active when the run ends, unless its budget was already zero; the stopping and exhaustion rules spend its entire budget. □

Theorem 6.3 (Two-sided settlement and individual rationality)**.** *The two-sided mechanism terminates, is exact-settlement feasible, and is individually rational. Specifically, when sell-Y is dominant,*

$$X_f \ge M, \qquad Y_f = \widetilde{C}_M(X_f) = p_0 M + C(X_f - M), \qquad 0 \le X_f - M < x_0. \tag{58}$$

For every reported profile, executed prices also satisfy

$$S_{Y,i} \ge p_0 R_{X,i} \quad (i \in \mathcal{I}_Y), \qquad R_{Y,i} \le p_0 S_{X,i} \quad (i \in \mathcal{I}_X). \tag{59}$$

Thus a sell-Y identity buys X at prices at least p_0, and a sell-X identity sells X at prices at most p_0.

Proof. When sell-Y is dominant, $D_Y \ge D_X$. The initial target is

$$\widetilde{T}_M(p_0, 0, 0) = M + Z(p_0) =: \Delta_0, \tag{60}$$

the length of the extended cost's initial linear segment. The total dominant budget is $B_0 = p_0 D_Y$. If the run stops at p_0, the stopping rule allocates $X_f = \min\{\Delta_0, B_0/p_0\}$: it clears the whole initial target when the budget suffices, and otherwise spends every budget on a prefix of that linear segment. Both Δ_0 and $B_0/p_0 = D_Y$ are at least M, so $X_f \ge M$.

If the run continues beyond p_0, its terminal allocation is at least Δ_0. To see this, recall the two settlement cases in the proof of Theorem 4.11. A fully cleared terminal chord has allocation at the rightmost chord endpoint, which is at or beyond the initial linear segment. A terminal point in a partially allocated lump lies on a linear segment of slope $p_f > p_0$, which is also beyond that initial segment. The boundary case $S = 0$ is a fully cleared chord. Thus the minority fill is absorbed in every case.

By Lemmas 6.1 and 6.2, the dominant run terminates and satisfies $Y_f = \widetilde{C}_M(X_f)$. Substituting $X_f \ge M$ gives (58). The minority supplies M units of X and receives $p_0 M$ units of Y; the remaining flows are $X_{\text{pool}} = X_f - M$ and $Y_{\text{pool}} = C(X_f - M)$. This is exactly Definition 2.2, with no deficit in either asset.

Dominant identities obey their reported budgets and pay at most their reported values per unit, by the one-sided rules. Minority identities receive $p_0 r_i \geq u_i r_i$. These facts give individual rationality on truthful profiles. They also show that buyers pay clock prices at least p_0, while sellers receive exactly p_0, proving (59) in this case.

Exchanging the assets proves the corresponding settlement and budget claims when sell-X is dominant. Sellers then pay at most their reciprocal value in the exchanged auction, so their original surplus $R_{Y,i} - u_i S_{X,i}$ is nonnegative. For $u_i = 0$ this is immediate. The ascending clock $p^{\mathrm{rev}} \geq 1/p_0$ pays sellers original prices $1/p^{\mathrm{rev}} \leq p_0$, while minority buyers pay exactly p_0.

Finally, if $D_Y = D_X = M$, the entire dominant budget buys exactly M units at p_0. The initial stopping rule spends every identity's budget, including those exiting at p_0, and the pool is unchanged. This also proves that the tie designation is immaterial. □

6.2 The Initial Fill and the Imbalance

Recall that $Z(p_0)$ is the value at p_0 of the marginal-supply function defined in (36).

Lemma 6.4 (Guaranteed allocation at the spot price)**.** *Suppose sell-Y is dominant, and let $\eta = D_Y - M$. At the initial price p_0, first set the residual supply to the initial target $S = \widetilde{T}_M(p_0, 0, 0) = M + Z(p_0)$. Before processing any identities that exit at p_0, the water level is*

$$h_0 = p_0 D_Y - p_0\Big(M + Z(p_0)\Big) = p_0\Big(\eta - Z(p_0)\Big) \leq p_0\eta. \tag{61}$$

Every eligible dominant identity receives at least

$$x_i(p_0) \geq \left(\frac{q_i}{p_0} - \eta\right)_+.$$

Consequently a truthful identity (V, Q), $V \geq p_0$, obtains utility at least $(V - p_0)(Q/p_0 - \eta)_+$.

Proof. Equation (61) follows from (60). Let B_E be the total budget of identities exiting at p_0. If the run continues, restoration lowers each active budget to at most $h^\star = h_0 - B_E \leq p_0\eta$, so its spot-price purchase is $(q_i - h^\star)_+/p_0$. An exiting identity receives nothing in this case, but $q_i \leq B_E < h_0 \leq p_0\eta$, so its claimed lower bound is zero. If the run stops, every active budget is spent. The total unspent exiting budget is $\max\{h_0, 0\}$, so each exiting identity spends at least $(q_i - \max\{h_0, 0\})_+$. This proves the allocation bound in all cases. All later truthful purchases have nonnegative surplus, proving the utility bound. □

Thus the imbalance measures how much of a dominant bidder's spot-price demand can remain unfilled. The pool's own initial linear segment can only improve this guarantee. This observation will bound the gain from changing which side is the minority.

6.3 The Value of Additional Spot-Price Supply

The same-direction Sybil theorem, Theorem 4.18, already shows that, for a fixed extended cost curve, a trader cannot benefit by splitting its sell-Y participation among

multiple identities or misreporting their values. Thus the new issue in the two-sided incentive proof is the effect of opposite-direction sell-X identities on the cost curve faced by the trader's merged sell-Y identity.

The proof in Section 6.4 first considers a strategic trader with true sell-Y type; the sell-X case follows by exchanging the assets. Suppose the truthful profile has sell-Y as the dominant side. If the trader submits opposite-direction sell-X identities and sell-Y remains dominant, those identities enlarge the minority fill from M to $M+E$, thereby lengthening the initial p_0-price segment of the extended cost curve. This additional supply may benefit the trader's merged sell-Y identity, but supplying the E units of X through its opposite-direction identities costs the trader $(V-p_0)E$ in surplus. Lemma 6.5 shows that the gain from the enlarged fill cannot exceed this cost. A deviation that changes which side is dominant is handled separately in Section 6.4.

Fix outside sell-Y reports and a true value $V \geq p_0$. Let $\mathcal{U}(M,Q)$ denote the utility of the single truthful identity (V,Q) in the one-sided run on $\widetilde{C}_M$. In this notation the fill is a parameter of the cost; no minority orders are part of this one-sided comparison.

Lemma 6.5 (Fill-shift bound)**.** *For all $M,E,Q \geq 0$,*

$$\mathcal{U}(M+E, Q+p_0E) \leq \mathcal{U}(M,Q) + (V-p_0)E.$$

The comparison gives the bidder both E extra units of initial supply and the p_0E needed to buy them. The lemma says that its utility can increase by no more than the surplus of buying those units at the spot price. Because the extra supply can change the whole auction path, the proof compares mark-to-market gains, as in the one-sided incentive proof.

Proof. If $V = p_0$, both utilities are zero. If $Q = 0$, then $\mathcal{U}(M,0) = 0$, and a budget of p_0E buying only at prices at least p_0 gives surplus at most $(V-p_0)E$. Hence assume $V > p_0$ and $Q > 0$.

Call the smaller-fill run 0 and the larger-fill run 1. Their costs are $C_0 := \widetilde{C}_M$ and $C_1 := \widetilde{C}_{M+E}$, and the focal identity k has budgets Q and $Q+p_0E$, respectively. All outsider reports N are the same. Use $T^r, h^r, \beta^r = Y^r + B^r$ for the state of run r, and use $\Gamma^r_k, \Gamma^r_N, W^r_N$ as in (44) and (45). After a run ends, allocations and payments stay fixed, effective budgets are zero, and its target is evaluated at the current comparison price.

The costs satisfy the translation identity

$$C_1(z+E) = C_0(z) + p_0E. \tag{62}$$

Consequently translating an auction state by (E, p_0E) translates its rightmost chord endpoint by E. Define the shift-adjusted gain gap of the focal identity and the outsider gain gap by

$$\mathrm{GainGap}_k := \Gamma^0_k - \Gamma^1_k + (p-p_0)E, \qquad \mathrm{GainGap}_N := \Gamma^1_N - \Gamma^0_N.$$

Both functions are locally absolutely continuous and vanish at p_0 by Lemma 4.15. Moreover,

$$\mathrm{GainGap}'_k = x^0_k - x^1_k + E, \qquad p\,\mathrm{GainGap}'_N = \mathrm{GainGap}_N + Y^1_N - Y^0_N, \tag{63}$$

almost everywhere. At $p = V$, the desired inequality is exactly $\mathrm{GainGap}_k(V) \geq 0$.

Write $\psi_p^r(z) := pz - C_r(z)$. The chord equality and (62) give

$$\mathrm{GainGap}_k - \mathrm{GainGap}_N = \psi_p^0(T^0) - \psi_p^1(T^1) + (p - p_0)E = \psi_p^1(T^0 + E) - \psi_p^1(T^1).$$

Both arguments in the last expression are on the decreasing branch of ψ_p^1: they are rightmost chord endpoints, with the first one translated as above. The same strict monotonicity used in the proof of Proposition 4.6 therefore implies

$$\begin{aligned} \mathrm{GainGap}_k \leq \mathrm{GainGap}_N &\implies T^1 \leq T^0 + E, \\ \mathrm{GainGap}_k \geq \mathrm{GainGap}_N &\implies T^1 \geq T^0 + E. \end{aligned} \tag{64}$$

Let p_1 be the terminal price of run 0, or V if that run continues to the focal identity's exit. Consider almost every $p \in (p_0, p_1)$. The outsider accounting from Lemma 4.17 uses only the common outsider reports and the single-run structural lemmas, so it gives

$$W_N^1 - W_N^0 \geq \mathrm{GainGap}_N / p. \tag{65}$$

There is equality while both runs continue. If run 1 has ended, the same terminal accounting gives $Y_N^1 \geq Y_N^0$.

When both runs continue, identical outsiders have had identical budgets cancelled, and the focal identity has not exited. Thus $\beta^1 - \beta^0 = p_0 E$. Since $h^r = \beta^r - C_r(T^r)$, the cost translation gives

$$h^0 - h^1 = C_1(T^1) - C_1(T^0 + E).$$

If $\mathrm{GainGap}_k \geq \mathrm{GainGap}_N$, then $T^1 \geq T^0 + E$, hence $h^1 \leq h^0$. The outsider payment formula (48) gives $Y_N^1 \geq Y_N^0$. This also holds when run 1 has ended, so (63) yields

$$\mathrm{GainGap}_k \geq \mathrm{GainGap}_N \quad \implies \quad \mathrm{GainGap}'_N \geq \mathrm{GainGap}_N / p. \tag{66}$$

For the other inequality, the supply invariant of the active focal identity in run 0 gives $x_k^0 \geq T^0 - W_N^0$, exactly as in the proof of Lemma 4.16. If the focal identity in continuing run 1 has never clinched, then $x_k^1 = 0$ and $\mathrm{GainGap}'_k \geq 0$. Otherwise clincher persistence, or target feasibility if that run has ended, gives $x_k^1 \leq T^1 - W_N^1$. Therefore, when $\mathrm{GainGap}_k \leq \mathrm{GainGap}_N$, (64) and (65) imply

$$\mathrm{GainGap}'_k \geq \min\{0, \mathrm{GainGap}_N / p\}. \tag{67}$$

Indeed, in the latter case the sharper bound is $\mathrm{GainGap}'_k \geq T^0 + E - T^1 + W_N^1 - W_N^0 \geq \mathrm{GainGap}_N / p$.

Equations (66) and (67) are precisely the two differential inequalities used in the first-crossing argument of Theorem 4.18. Applying that already proved argument to $\min\{\mathrm{GainGap}_k, \mathrm{GainGap}_N\}$, which starts at zero, gives $\mathrm{GainGap}_k, \mathrm{GainGap}_N \geq 0$ through p_1.

If $p_1 = V$, this proves the claim. Otherwise run 0 ended below V, so its focal identity spent all of Q. No focal budget has been cancelled in run 1 below V; write b_k^1 for its remaining budget at p_1, taking it to be zero if run 1 has ended. The definition of $\mathrm{GainGap}_k$ now gives

$$0 \leq \mathrm{GainGap}_k(p_1) = p_1\Big(x_k^0(p_1) - x_k^1(p_1) + E\Big) - b_k^1.$$

Every later unit in run 1 costs at least p_1, so its focal allocation can never exceed $x_k^0(p_1) + E$. Hence $\mathrm{GainGap}'_k \geq 0$ from p_1 to V, and $\mathrm{GainGap}_k(V) \geq 0$ follows. □

6.4 Sybil-Robust Incentive Compatibility Across Directions

Theorem 6.6 (Two-sided Sybil-robust incentive compatibility)**.** *The two-sided AMM clinching mechanism satisfies Sybil-robust incentive compatibility (Definition 2.6) for the full strategy space in Definition 2.4.*

Proof. Fix a physical trader k and all reports of the other traders. Truthful utility is finite and nonnegative by Theorem 6.3, so a deviation giving utility $-\infty$ cannot improve it. For all other deviations we compare the linear surplus of the aggregate net flows, as required by (5) and (6).

Eligible true sell-Y type. Suppose that trader k has type (V, Q), with $V \geq p_0$. Remove ineligible identities from the deviation, since they have no effect. Let

$$Q^{\mathrm{dev}} := \sum_{i \in \mathcal{I}_Y(k) \cap \mathcal{E}_Y} q_i \leq Q$$

be trader k's aggregate eligible sell-Y budget in the deviating strategy, and let $e := S_X(k)$ be the amount of X actually delivered by its sell-X identities. Recall from (4) that $\Delta_{X,k}$ and $\Delta_{Y,k}$ are trader k's aggregate net changes in its holdings of X and Y. The executed-price inequalities (59) imply

$$V\Delta_{X,k} + \Delta_{Y,k} \leq (V - p_0)\left(\frac{Q^{\mathrm{dev}}}{p_0} - e\right). \tag{68}$$

For clarity, if its sell-Y identities spend $s \leq Q^{\mathrm{dev}}$, their allocation is at most s/p_0, so their surplus is at most $(V/p_0 - 1)s \leq (V - p_0)Q^{\mathrm{dev}}/p_0$. Its opposite-direction identities receive at most $p_0 e$ for an asset worth Ve to this same physical trader. Combining these two contributions proves the deviation-surplus bound in (68). In particular, the case $V = p_0$ is immediate: every deviation has nonpositive linear surplus and truthfulness gives zero.

Suppose $V > p_0$. If sell-X is dominant in the truthful profile, the focal identity spends all of Q at p_0 and obtains $(V - p_0)Q/p_0$. Equation (68), with $Q^{\mathrm{dev}} \leq Q$ and $e \geq 0$, shows that no deviation can exceed this utility.

It remains to consider a truthful profile in which sell-Y is dominant. Let M be the total eligible outside sell-X budget and let $\eta = D_Y - M$. The truthful utility is $\mathcal{U}(M, Q)$, and Lemma 6.4 gives

$$\mathcal{U}(M, Q) \geq (V - p_0)(Q/p_0 - \eta)_+. \tag{69}$$

There are two cases.

- *The deviation leaves sell-Y dominant.* All eligible opposite-direction identities are then filled in full at p_0. Write $E = e$ for their total X-budget. The dominant cost becomes $\widetilde{C}_{M+E}$. On this fixed cost, Theorem 4.18 and Lemma 6.1 bound the group's sell-Y surplus by that of a single truthful identity with budget $Q + p_0 E$, since $Q^{\mathrm{dev}} \leq Q \leq Q + p_0 E$. After accounting for the opposite-direction deliveries, the full linear surplus is at most

  $$\mathcal{U}(M + E, Q + p_0 E) - (V - p_0)E \leq \mathcal{U}(M, Q),$$

  where the last step is Lemma 6.5. The larger budget here is only an upper bound used in the proof; the admissible deviation still has the original cap $Q^{\mathrm{dev}} \leq Q$.

- *The deviation makes sell-X dominant.* Its new total demand is $D_Y^{\mathrm{dev}} = D_Y - Q/p_0 + Q^{\mathrm{dev}}/p_0$. By the exchanged version of Theorem 6.3, the dominant sell-X identities deliver at least D_Y^{dev} units of X to cover that minority fill. The outside sell-X identities can deliver at most M, hence

$$e \geq D_Y^{\mathrm{dev}} - M = Q^{\mathrm{dev}}/p_0 - Q/p_0 + \eta.$$

  Combining this with (68) gives linear surplus at most $(V - p_0)(Q/p_0 - \eta)$, which is bounded above by the truthful utility in (69). This case also includes a change of sides caused solely by withholding same-direction budget.

Eligible true sell-X type. First suppose $0 < U \leq p_0$, and exchange the assets. The trader's truthful value and budget in the exchanged auction are $(1/U, R)$. Admissibility becomes exactly the sell-Y constraint already considered: the same-direction budgets sum to at most R, while the opposite budgets are unrestricted. Its linear surplus in the exchanged numeraire is

$$\frac{\Delta_{Y,k} + U\Delta_{X,k}}{U},$$

a positive multiple of its original surplus. Thus the preceding proof applies. Any zero outside reservation reports can be represented by a common finite clock value above the bounds for the runs being compared, using Lemma 6.2.

For $U = 0$, take true values $\varepsilon > 0$ tending to zero, with the same budget R and fixed outside reports and deviation. For all sufficiently small ε, the truthful report (ε, R) produces exactly the outcome of $(0, R)$: if it is minority its fill is unchanged, and if it is dominant its reciprocal value exceeds the finite clock bound. The inequality just proved for linear surpluses is $R_Y^{\mathrm{tr}} - \varepsilon S_X^{\mathrm{tr}} \geq \Delta_{Y,k}^{\mathrm{dev}} + \varepsilon\Delta_{X,k}^{\mathrm{dev}}$. Letting $\varepsilon \downarrow 0$ proves the required bound for every finite-utility deviation of a zero-reservation type as well.

Ineligible true types. Finally, although our standing convention considers eligible true types, the definition also quantifies over ineligible ones. Summing (59) over a physical trader's identities gives, under every strategy,

$$\Delta_{Y,k} \leq -p_0\Delta_{X,k}. \tag{70}$$

A sell-Y type with $V < p_0$ has nonpositive linear surplus when $\Delta_{X,k} \geq 0$. When $\Delta_{X,k} < 0$, finite utility requires $\Delta_{Y,k} \leq 0$, so its surplus is again nonpositive. A sell-X type with $U > p_0$ has surplus at most $(U - p_0)\Delta_{X,k} \leq 0$ when $\Delta_{X,k} \leq 0$; if $\Delta_{X,k} > 0$, (70) makes the trade strictly opposite to its type and its utility is $-\infty$. Truthful ineligible reports receive zero. This completes the proof for every true type and for the stated net-flow utility functions. □

The two cases explain why opposite-direction identities do not help. If they remain on the minority side, their full delivery costs the trader at least the extra utility made possible by the enlarged fill. If they change which side is dominant, conservation forces enough actual delivery to offset the improvement in the trader's buying price. Both comparisons value every identity's trades at the physical trader's true value.

6.5 Weak Pareto Optimality for Eligible Bids

Theorem 6.7 (Two-sided weak Pareto optimality)**.** *Under truthful reporting, the two-sided AMM clinching outcome is weakly Pareto optimal for eligible bids in the sense of Definition 2.7.*

Proof. Use the holdings and coefficients (H_i^X, H_i^Y, t_i) already defined in (7). We first show that there is a positive cutoff λ such that

$$H_i^Y > 0 \implies t_i \le \lambda, \qquad H_i^X > 0 \implies t_i \ge \lambda. \tag{71}$$

Thus everyone who can pay Y values X no more highly than anyone who can supply it.

When sell-Y is dominant, let

$$\lambda := \begin{cases} \max\{V_i : Q_i - S_{Y,i} > 0,\ i \in \mathcal{E}_{\mathrm{Y}}\}, & \text{if this set is nonempty,} \\ p_0, & \text{otherwise.} \end{cases}$$

Minority sell-X users have holdings $(0, p_0 R_i)$ and values $U_i \le p_0 \le \lambda$. Dominant users with remaining Y have values at most λ by definition. Every holder of X is a dominant user; its value is at least λ by the first part of Lemma 4.12 applied to $\widetilde{C}_M$, or by eligibility if no dominant user has residual budget. This proves (71) in this case.

When sell-X is dominant, let

$$\lambda := \begin{cases} \min\{U_i : R_i - S_{X,i} > 0,\ i \in \mathcal{E}_{\mathrm{X}}\}, & \text{if this set is nonempty,} \\ p_0, & \text{otherwise.} \end{cases}$$

A zero-reservation dominant user spends all of its X-budget by Lemma 6.2, so $0 < \lambda \le p_0$. Minority sell-Y users have holdings $(Q_i/p_0, 0)$ and values $V_i \ge p_0 \ge \lambda$. Every other holder of X has value at least λ by definition. A dominant user j holding positive Y must have $U_j \le U_i$ for every dominant user i with residual X: for positive reservation values this is the first terminal-certificate statement with reciprocal values, and for $U_j = 0$ it is immediate. If no such residual user exists, eligibility gives $U_j \le p_0 = \lambda$. Thus (71) holds in this case too.

The internal-trade argument in Theorem 4.13 now applies to all eligible users together. To spell out its use of the cutoff, a user paying Y can pay at most λ times the X it receives while weakly improving its utility. A user supplying X requires at least λ times that quantity in Y. Conservation of both tokens forces equality in all these bounds and leaves every utility unchanged. Hence there is no strict Pareto improvement through internal trade, even when the trading subset includes both original directions.

It remains to check each user's permitted same-direction pool trade. When sell-Y is dominant, set $z := X_f - M \ge 0$. A dominant user with unspent Y satisfies

$$V_i \le \widetilde{C}'_{M,+}(X_f) = a(z)$$

by the second terminal-certificate statement. From the settled pool state, receiving another $\delta > 0$ units of X costs $C(z+\delta) - C(z) \ge a(z)\delta$, so that user cannot gain. Minority sell-X users have no remaining X to tender in their own direction, because their endowments were filled in full.

When sell-X is dominant, write $w := \sum_{i\in\mathcal{E}_X} R_{Y,i} - \sum_{i\in\mathcal{E}_Y} Q_i \geq 0$ for the net Y released by the pool, and put $a^{\mathrm{rev}} := (C^{\mathrm{rev}})'_+$. A dominant user with residual X has $U_i > 0$, and the exchanged terminal certificate gives

$$1/U_i \leq a^{\mathrm{rev}}(w).$$

Receiving an additional $\delta > 0$ units of Y costs at least $C^{\mathrm{rev}}(w+\delta) - C^{\mathrm{rev}}(w) \geq a^{\mathrm{rev}}(w)\delta$ units of X. Its utility change is therefore at most $(1 - U_i a^{\mathrm{rev}}(w))\delta \leq 0$. Minority sell-$Y$ users have spent all of their Y-budgets, so they cannot make an additional trade in their own direction. This proves the second clause of Definition 2.7 and completes the proof. □

7 Impossibility with Budget Overreporting

The positive incentive results above restrict a trader's aggregate declared budget in its true direction to its actual budget. We now show that this restriction is essential. Suppose instead that a trader may declare a larger budget, with the deviation regarded as feasible whenever the amount actually paid does not exceed its true budget. Even without Sybil identities or opposite-direction orders, this enlarged strategy space is incompatible with the other desired properties.

Under the enlarged strategy space considered here, a true eligible type (V, Q) may replace its report by any single finite eligible report (v, q). If that report produces (x, y), the deviation has finite utility precisely when $y \leq Q$. Incentive compatibility with budget overreporting therefore requires

$$y \leq Q \quad \Longrightarrow \quad V x^{\mathrm{tr}} - y^{\mathrm{tr}} \geq V x - y,$$

where $(x^{\mathrm{tr}}, y^{\mathrm{tr}})$ is the truthful outcome. In particular, when the mechanism does not require advance escrow of the entire declared budget, budget overreporting becomes possible as long as its realized payment remains affordable.

Theorem 7.1 (Budget-overreporting impossibility)**.** *For a constant-product AMM, there is no deterministic mechanism that, on every profile of two eligible sell-Y users, simultaneously satisfies:*

1. *individual rationality (Definition 2.3);*
2. *exact settlement (Definition 2.2);*
3. *both clauses of weak Pareto optimality in Definition 2.7; and*
4. *incentive compatibility against single-identity eligible value and budget misreports, including budget overreports whose realized payment does not exceed the true budget.*

All true types and reports used in the proof are eligible and have finite values and budgets.

We stress that this impossibility holds in a strong sense. It assumes neither symmetry nor resistance to Sybil or opposite-direction deviations, and it already applies to the much smaller class of deviations that replace one sell-Y report by another. As

a practical implication, the impossibility holds even when the underlying consensus protocol provides fair sequencing [dec, KZGJ20, KDK22, KDL+23, Kur20, ZSC+20] and censorship resilience [AER25, GNR25, foc].

7.1 Normalization and Basic Consequences

By rescaling, we may assume without loss of generality that $x_0 = y_0 = 1$, and hence $p_0 = 1$, throughout the proof. The pool then releases

$$F(y) := C^{-1}(y) = \frac{y}{1+y}, \qquad F'(y) = \frac{1}{(1+y)^2},$$

and a sell-Y value is eligible exactly when $V \geq 1$.

For $V > 1$, define

$$\mathrm{Util}^{\mathrm{pool}}(V, y) := VF(y) - y, \qquad y^\star(V) := \sqrt{V} - 1, \qquad \bar{y}(V) := V - 1.$$

Here $\mathrm{Util}^{\mathrm{pool}}(V, y)$ is the utility of a value-V user that receives all pool output generated by a payment y. It increases up to its unique maximizer $y^\star(V)$, then decreases; its two zeros are 0 and $\bar{y}(V)$. In particular,

$$0 < y^\star(V) < \bar{y}(V), \qquad \mathrm{Util}^{\mathrm{pool}}\Big(V, y^\star(V)\Big) = (\sqrt{V} - 1)^2.$$

Set $y^\star(1) = \bar{y}(1) = 0$.

The first lemma is a strict priority property. A higher-valued user that still has some Y available could profitably purchase any allocation held by a lower-valued user. Weak Pareto optimality therefore prevents the lower value from receiving anything.

Lemma 7.2 (Internal-trade priority)**.** *Consider a truthful profile of two eligible sell-Y users. Denote their values and budgets by (V_1, q_1) and (V_2, q_2), and their respective allocations and payments by (x_1, y_1) and (x_2, y_2). If $V_1 > V_2$ and $y_1 < q_1$, then $x_2 = y_2 = 0$.*

Proof. Suppose $x_2 > 0$. Choose a price $P \in (V_2, V_1)$ and a sufficiently small $\delta > 0$ such that $P\delta \leq q_1 - y_1$ and $\delta < x_2$. Let user 1 give $P\delta$ units of Y to user 2 in exchange for δ units of X. The utility gains are $(V_1 - P)\delta > 0$ and $(P - V_2)\delta > 0$, and both users retain nonnegative holdings. This contradicts the internal-trade clause of weak Pareto optimality. Hence $x_2 = 0$, and individual rationality with $V_2 > 0$ forces $y_2 = 0$. □

We will repeatedly use two other consequences of individual rationality, settlement, and weak Pareto optimality. Write $Y = y_1 + y_2$. First, if either user has unspent budget, a small additional payment to the terminal pool cannot be profitable, so

$$\begin{aligned} y_1 < q_1 \quad &\Longrightarrow \quad V_1 F'(Y) \leq 1, \\ y_2 < q_2 \quad &\Longrightarrow \quad V_2 F'(Y) \leq 1. \end{aligned} \tag{72}$$

Second, if $V_{\max} := \max\{V_1, V_2\} > 1$, individual rationality and exact settlement give

$$F(Y) = x_1 + x_2 \geq \frac{y_1}{V_1} + \frac{y_2}{V_2} \geq \frac{Y}{V_{\max}}, \qquad \text{and hence} \qquad Y \leq \bar{y}(V_{\max}). \tag{73}$$

We next derive several standard consequences of value incentive compatibility when the reported budget is held fixed. In particular, incentive compatibility implies the continuity properties used later; we do not separately assume that the mechanism or its allocation and payment rules are continuous.

Lemma 7.3 (Fixed-budget Myerson lemma [Mye81])**.** *Fix one user's declared budget q and the other user's report. Let $(x(V), y(V))$ be its outcome when its reported value is V, and put* $\mathrm{Util}(V) := Vx(V) - y(V)$*. On the eligible interval $[1, \infty)$, the functions x, y, and* Util *are nondecreasing, and* Util *is nonnegative, convex, and continuous (with one-sided continuity at 1). Moreover, the standard single-parameter payment identity and its normalized-utility form are, for $1 \le V < W$,*

$$\mathrm{Util}(W) - \mathrm{Util}(V) = \int_V^W x(t)\,\mathrm{d}t, \qquad \frac{\mathrm{Util}(W)}{W} - \frac{\mathrm{Util}(V)}{V} = \int_V^W \frac{y(t)}{t^2}\,\mathrm{d}t. \tag{74}$$

Proof. For eligible values $1 \le V < W$, incentive compatibility in both directions gives

$$x(W) \ge x(V), \qquad V\Big(x(W) - x(V)\Big) \le y(W) - y(V) \le W\Big(x(W) - x(V)\Big).$$

Thus allocation and payment are nondecreasing. Moreover,

$$\mathrm{Util}(V) = \sup_{v \ge 1}\{Vx(v) - y(v)\},$$

with the supremum attained at $v = V$. It is therefore a finite convex nondecreasing function, and hence continuous; individual rationality makes it nonnegative.

The same incentive inequalities bound $\mathrm{Util}(W) - \mathrm{Util}(V)$ between $(W-V)x(V)$ and $(W-V)x(W)$. Summing over partitions and taking upper and lower sums gives the first identity in (74). Thus Util is locally absolutely continuous and $\mathrm{Util}'(V) = x(V)$ almost everywhere. Since $\mathrm{Util}(V) = Vx(V) - y(V)$, it follows almost everywhere that

$$\frac{\mathrm{d}}{\mathrm{d}V}\left(\frac{\mathrm{Util}(V)}{V}\right) = \frac{Vx(V) - \mathrm{Util}(V)}{V^2} = \frac{y(V)}{V^2}.$$

Integrating proves the second identity. □

The next lemma establishes the spot-price normalization needed below using only eligible reports: when one user's value equals the initial spot price, that user receives nothing. Intuitively, such a user gains nothing from the pool, whose average price exceeds the spot price, so it could gain only by being subsidized by the other user; weak Pareto optimality alone does not exclude this when the other user has exhausted its budget. The proof instead squeezes the other user's utility: incentive compatibility, through the normalized-utility identity of Lemma 7.3, guarantees it at least the utility it would obtain by trading alone against the pool, whereas feasibility caps it at that amount, with a strict loss whenever the spot-value user receives any allocation.

Lemma 7.4 (A spot-value user receives zero)**.** *For any budgets $q, Q \ge 0$ and any eligible value $V \ge 1$, consider the profile*

$$((V, q), (1, Q)).$$

The spot-value user receives $(x_2, y_2) = (0, 0)$, while the first user receives the sole-user optimum

$$y_1 = \min\{q, y^\star(V)\}, \qquad x_1 = F(y_1).$$

The same conclusion holds with the two user positions interchanged.

Proof. Fix the second report $(1, Q)$, vary the first user's reported value $V \geq 1$, and write its outcome as $(x_1(V), y_1(V))$ and its reported utility as $\mathrm{Util}_1(V) := Vx_1(V) - y_1(V)$. At $V = 1$, both values equal the spot value. Individual rationality and exact settlement imply $F(Y) = x_1 + x_2 \geq Y$. Since $F(Y) < Y$ for $Y > 0$, both users receive zero and $\mathrm{Util}_1(1) = 0$.

Now let $V > 1$. If the first user does not exhaust its budget, Lemma 7.2 gives $x_2 = y_2 = 0$, and (72) gives $VF'(y_1(V)) \leq 1$, or equivalently $y_1(V) \geq y^\star(V)$. If it does exhaust its budget, $y_1(V) = q$. Consequently

$$y_1(V) \geq \min\{q, y^\star(V)\}.$$

The normalized-utility identity in (74) now gives

$$\begin{aligned}\frac{\mathrm{Util}_1(V)}{V} &\geq \int_1^V \frac{\min\{q, y^\star(t)\}}{t^2}\,\mathrm{d}t \\ &= \max_{0\leq z\leq q}\left\{F(z) - \frac{z}{V}\right\}.\end{aligned}$$

For the equality, the maximizer on the right is $z = \min\{q, y^\star(V)\}$; differentiating both sides with respect to V, starting from their common value zero at $V = 1$, gives the same integrand.

Conversely, individual rationality for the spot-value user gives $x_2 \geq y_2$. Exact settlement and $F' \leq 1$ therefore imply

$$\begin{aligned}\frac{\mathrm{Util}_1(V)}{V} &= F(y_1 + y_2) - x_2 - \frac{y_1}{V} \\ &\leq F(y_1 + y_2) - y_2 - \frac{y_1}{V} \\ &\leq F(y_1) - \frac{y_1}{V} \\ &\leq \max_{0\leq z\leq q}\left\{F(z) - \frac{z}{V}\right\}.\end{aligned}$$

The second inequality is strict when $y_2 > 0$. Equality with the lower bound forces $y_2 = 0$, then $x_2 = 0$, and strict concavity of F forces $y_1 = \min\{q, y^\star(V)\}$. Interchanging the fixed user positions gives the same proof; no symmetry assumption is needed. □

Consequently, no eligible report can buy X below the spot price: a user with the spot value, which obtains zero utility by Lemma 7.4, could otherwise profit by imitating that report.

Corollary 7.5 (Spot-price payment bound)**.** *Every profile of two eligible users satisfies*

$$x_1 \leq y_1 \qquad \textit{and} \qquad x_2 \leq y_2.$$

In particular, a user that pays zero receives zero.

Proof. Hold user 2's eligible report fixed. If user 1 had the spot value 1 and its current budget, Lemma 7.4 would give it zero utility. It can instead submit its current eligible value report without changing its budget. Incentive compatibility for the spot-value true type therefore gives $0 \geq x_1 - y_1$. Interchanging the two user positions gives $0 \geq x_2 - y_2$. □

7.2 Two Large-Budget Comparisons

We now establish two complementary facts. In the first, a large declared budget belongs to the lower-valued user. In the second, it belongs to the higher-valued user. Together they show that a declared budget can control the allocation even when most of that budget is never paid.

Lemma 7.6 below considers the former case. It shows that a lower-valued user with a large budget sets the price for a budget-constrained higher-valued user, much as a second price would: the higher-valued user spends its entire budget at a unit price equal to the lower value. The lower-valued user takes the remaining supply at a strictly positive profit, and its payment stays bounded no matter how large its declared budget is.

Lemma 7.6 (Large budget on the lower-valued user)**.** *Fix $V_1 > 1$, $0 < Q_1 < \bar{y}(V_1)$, and $Q^{\text{large}} > \bar{y}(V_1)$, and put*

$$V_{\text{cut}} := \frac{Q_1}{F(Q_1)} = 1 + Q_1,$$

so that $1 < V_{\text{cut}} < V_1$. For every $V_2 \in (V_{\text{cut}}, V_1)$, the profile $((V_1, Q_1), (V_2, Q^{\text{large}}))$ satisfies

$$y_1 = Q_1, \qquad x_1 = \frac{Q_1}{V_2}, \qquad y_2 \le \bar{y}(V_2) - Q_1, \qquad V_2 x_2 - y_2 > 0. \tag{75}$$

Proof. Fix V_2, vary the first user's value $v \in [1, V_1]$ while holding its budget at Q_1, and keep the second report (V_2, Q^{large}) fixed. Write $(x_1(v), y_1(v))$ for the first user's outcome and $\text{Util}_1(v) := v x_1(v) - y_1(v)$. By (73), total payment never exceeds $\bar{y}(V_1) < Q^{\text{large}}$, so the second user always has unspent budget.

When $v < V_2$, internal-trade priority gives $(x_1(v), y_1(v)) = (0, 0)$; continuity therefore gives $\text{Util}_1(V_2) = 0$. Suppose $y_1(v_0) < Q_1$ for some $v_0 > V_2$. Payment monotonicity then gives $y_1(v) < Q_1$ throughout a right neighborhood of V_2. The first user is the higher-valued user there and also has unspent budget, so priority gives the second user zero. Exact settlement and the pool condition imply

$$x_1(v) = F(y_1(v)), \qquad y_1(v) \ge y^\star(v), \qquad \text{Util}_1(v) = \text{Util}^{\text{pool}}\Big(v, y_1(v)\Big).$$

The monotone limit $y_{\text{lim}} := \lim_{v \downarrow V_2} y_1(v)$ consequently satisfies

$$y^\star(V_2) \le y_{\text{lim}} < Q_1 < \bar{y}(V_2).$$

Continuity of Util_1 would give $\text{Util}^{\text{pool}}(V_2, y_{\text{lim}}) = \text{Util}_1(V_2) = 0$, contradicting the fact that $\text{Util}^{\text{pool}}(V_2, \cdot)$ is strictly positive between its two zeros. Hence $y_1(v) = Q_1$ for every $v \in (V_2, V_1]$.

With payment fixed at Q_1, incentive compatibility forces allocation to be constant on this interval, say $x_1(v) = x_{\text{const}}$. Taking $v \downarrow V_2$ in $\text{Util}_1(v) = v x_{\text{const}} - Q_1$ gives $V_2 x_{\text{const}} - Q_1 = \text{Util}_1(V_2) = 0$, so $x_{\text{const}} = Q_1/V_2$. This proves the first two claims in (75). Individual rationality for user 2 and exact settlement give

$$F(Q_1 + y_2) = \frac{Q_1}{V_2} + x_2 \ge \frac{Q_1 + y_2}{V_2},$$

and therefore $Q_1 + y_2 \le \bar{y}(V_2)$.

It remains to show that user 2 has strictly positive utility. Keep the first report (V_1, Q_1) fixed, vary user 2's reported value v while holding its declared budget at Q^{large}, and write its reported utility $vx_2 - y_2$ as $\text{Util}_2(v)$. If $\text{Util}_2(V_2) = 0$, nonnegativity and monotonicity give $\text{Util}_2(v) = 0$ for every $v \in (V_{\text{cut}}, V_2)$. Choose such a v. The conclusions already proved give $y_1 = Q_1$ and $x_1 = Q_1/v$. Zero utility for user 2 and exact settlement then give

$$F(Q_1 + y_2) = \frac{Q_1 + y_2}{v}, \qquad y_2 = \bar{y}(v) - Q_1 > 0.$$

A true type (V_2, Q^{large}) could instead report (v, Q^{large}) and obtain $(V_2 - v)x_2 > 0$, contradicting incentive compatibility. Thus $\text{Util}_2(V_2) > 0$. □

Lemma 7.7 below considers the mirror case, in which the higher-valued user has a large budget. It shows that this user effectively trades alone against the pool, while the lower-valued user receives nothing. The only thing the mechanism can do to the higher-valued user is impose a minimum purchase, and incentive compatibility keeps the resulting overpayment small when the lower-valued user's budget is small.

Lemma 7.7 (Large budget on the higher-valued user)**.** *Fix $V_1 > V_2 > 1$, $Q_2 > 0$, and $Q^{\text{large}} > \bar{y}(V_1)$. For $v \in [V_2, V_1]$, consider the profile $((v, Q^{\text{large}}), (V_2, Q_2))$, and write the first user's outcome as $(x_1(v), y_1(v))$. For $v > V_2$, user 2 receives zero and*

$$x_1(v) = F(y_1(v)), \qquad y_1(v) \ge y^\star(v).$$

The limit $y_{\text{lim}} := \lim_{v \downarrow V_2} y_1(v)$ exists and satisfies

$$y_{\text{lim}} \ge y^\star(V_2), \qquad \text{Util}^{\text{pool}}(V_2, y_{\text{lim}}) \ge \text{Util}^{\text{pool}}\Big(V_2, y^\star(V_2)\Big) - V_2 Q_2, \tag{76}$$

and, for every $v \in (V_2, V_1]$,

$$y_1(v) = \max\{y_{\text{lim}}, y^\star(v)\}. \tag{77}$$

Proof. The total-payment bound gives $Y \le \bar{y}(V_1) < Q^{\text{large}}$, so the first user never exhausts its declared budget. For $v > V_2$, internal-trade priority therefore gives user 2 zero. Settlement and the pool condition yield the two displayed assertions. Monotonicity and boundedness of y_1 give the limit $y_{\text{lim}} \ge y^\star(V_2)$. If $\text{Util}_1(v) := vx_1(v) - y_1(v)$, continuity gives

$$\text{Util}_1(V_2) = \lim_{v \downarrow V_2} \text{Util}^{\text{pool}}\Big(v, y_1(v)\Big) = \text{Util}^{\text{pool}}(V_2, y_{\text{lim}}).$$

To lower-bound this utility, choose a finite eligible value v_{aux} so large that

$$v_{\text{aux}} F'\Big(y^\star(V_2) + Q_2\Big) > 1.$$

A true type (V_2, Q^{large}) can deviate to the report $(v_{\text{aux}}, y^\star(V_2))$. In the resulting profile $((v_{\text{aux}}, y^\star(V_2)), (V_2, Q_2))$, the first user must pay all $y^\star(V_2)$: otherwise it would have unspent budget and (72), together with $Y < y^\star(V_2) + Q_2$, would imply

$$1 \ge v_{\text{aux}} F'(Y) \ge v_{\text{aux}} F'\Big(y^\star(V_2) + Q_2\Big) > 1.$$

By Corollary 7.5, user 2 receives at most $x_2 \le y_2 \le Q_2$. Exact settlement therefore gives the deviating user at least $F(y^\star(V_2)) - Q_2$ units of X. The deviation is affordable because it pays $y^\star(V_2) < Q^{\text{large}}$, and incentive compatibility yields

$$\begin{aligned}\text{Util}^{\text{pool}}(V_2, y_{\text{lim}}) &= \text{Util}_1(V_2) \\ &\ge V_2\Big(F(y^\star(V_2)) - Q_2\Big) - y^\star(V_2) \\ &= \text{Util}^{\text{pool}}\Big(V_2, y^\star(V_2)\Big) - V_2 Q_2,\end{aligned}$$

which proves (76). Notice that v_{aux} is finite; the proof does not use an infinite value report.

It remains to identify the payment path. Payment monotonicity already gives $y_1(v) \ge y_{\text{lim}}$, and the pool condition gives $y_1(v) \ge y^\star(v)$. The function y_1 is continuous on $(V_2, V_1]$: its one-sided limits exist by monotonicity, and continuity of $\text{Util}_1(v) = \text{Util}^{\text{pool}}\Big(v, y_1(v)\Big)$, together with strict decrease of $\text{Util}^{\text{pool}}(v, \cdot)$ on $[y^\star(v), \infty)$, forces those limits to agree.

If $y_1(v) > \max\{y_{\text{lim}}, y^\star(v)\}$ at some v, continuity and the definition of y_{lim} provide $v' \in (V_2, v)$ such that

$$\max\{y_{\text{lim}}, y^\star(v)\} < y_1(v') < y_1(v).$$

Both reports give the first user the entire pool output. Because $\text{Util}^{\text{pool}}(v, \cdot)$ strictly decreases above $y^\star(v)$, a true value v would strictly prefer the report v', contradicting incentive compatibility. This proves (77). □

7.3 The Contradiction

The proof constructs a truthful profile of two eligible users in which each user has an affordable budget overreport, that is, one whose realized payment does not exceed its true budget. By Lemma 7.7, the first user's overreport guarantees it utility 1, which is the entire surplus that the batch can generate. By Lemma 7.6, the second user's overreport guarantees it strictly positive utility. Incentive compatibility requires the truthful outcome to give each user at least what its overreport guarantees, and these two guarantees together exceed the available surplus.

Proof of Theorem 7.1. In normalized units, consider the truthful profile

$$(V_1, Q_1) = (4, 1), \qquad (V_2, Q_2) = \left(\frac{100}{49}, \frac{2}{49}\right),$$

and let $Q^{\text{large}} = 4$ be the larger budget used in the two deviations below. Both values are strictly eligible. Write $\text{Util}_1^{\text{tr}} := V_1 x_1^{\text{tr}} - y_1^{\text{tr}}$ and $\text{Util}_2^{\text{tr}} := V_2 x_2^{\text{tr}} - y_2^{\text{tr}}$.

The first user can safely overreport its budget. Apply Lemma 7.7; its hypotheses hold because $V_1 > V_2 > 1$ and $Q^{\text{large}} = 4 > \bar{y}(V_1) = 3$. We have

$$y^\star(V_2) = \frac{3}{7}, \qquad \text{Util}^{\text{pool}}\Big(V_2, y^\star(V_2)\Big) = \frac{9}{49}, \qquad \text{Util}^{\text{pool}}(V_2, 1) = \frac{1}{49}.$$

Consequently,

$$\text{Util}^{\text{pool}}(V_2, y_{\text{lim}}) \ge \frac{9}{49} - \frac{100}{49} \cdot \frac{2}{49} = \frac{241}{2401} > \frac{1}{49} = \text{Util}^{\text{pool}}(V_2, 1).$$

Since $y_{\lim} \geq y^\star(V_2)$ and $\mathrm{Util}^{\mathrm{pool}}(V_2, \cdot)$ strictly decreases after its maximizer, this implies $y_{\lim} < 1$. Equation (77) at $v = V_1 = 4$ therefore gives

$$y_1(V_1) = \max\{y_{\lim}, y^\star(4)\} = 1.$$

Thus, if user 1 reports $(V_1, Q^{\mathrm{large}}) = (4, 4)$, it actually pays exactly its true budget $Q_1 = 1$, receives $F(1) = 1/2$, and obtains utility 1. Incentive compatibility requires

$$\mathrm{Util}_1^{\mathrm{tr}} \geq 1. \tag{78}$$

The second user's truthful utility must be zero. Let $Y^{\mathrm{tr}} = y_1^{\mathrm{tr}} + y_2^{\mathrm{tr}}$. Exact settlement and $V_1 > V_2$ give

$$\begin{aligned}\mathrm{Util}_1^{\mathrm{tr}} + \mathrm{Util}_2^{\mathrm{tr}} &= V_1 F(Y^{\mathrm{tr}}) - Y^{\mathrm{tr}} - (V_1 - V_2)x_2^{\mathrm{tr}} \\ &\leq \mathrm{Util}^{\mathrm{pool}}(V_1, Y^{\mathrm{tr}}) \leq \mathrm{Util}^{\mathrm{pool}}\Big(V_1, y^\star(V_1)\Big) = 1.\end{aligned}$$

Together with (78) and individual rationality, this forces $\mathrm{Util}_2^{\mathrm{tr}} = 0$.

The second user can also safely overreport its budget. Now let user 2 report $(V_2, Q^{\mathrm{large}})$, keeping user 1 at (V_1, Q_1). The hypotheses of Lemma 7.6 hold because

$$V_{\mathrm{cut}} = \frac{Q_1}{F(Q_1)} = 2 < V_2 < V_1, \qquad Q^{\mathrm{large}} = 4 > \bar{y}(V_1) = 3.$$

The lemma gives user 2 strictly positive utility, while its realized payment satisfies

$$y_2 \leq \bar{y}(V_2) - Q_1 = \frac{51}{49} - 1 = \frac{2}{49} = Q_2.$$

This deviation is therefore affordable under its true budget and strictly improves upon its truthful utility of zero, a contradiction.

□

Only the two deviations in the final contradiction overreport a budget. Every preparatory incentive comparison keeps the budget fixed or reports a smaller one. Both overreports keep the value truthful and realize a payment within the true budget. This pinpoints the obstruction: a declared budget can influence priority and allocation even when the mechanism never collects the overstated portion.

Finally, the theorem also rules out a two-sided mechanism with the same four properties. Restrict such a mechanism to the two sell-Y profiles used above. Exact settlement becomes $x_1 + x_2 = F(y_1 + y_2)$, both weak-Pareto clauses remain applicable, and every deviation in the proof is still an available single sell-Y deviation. Thus the restricted mechanism would contradict Theorem 7.1. The aggregate true-budget cap in Definition 2.4 excludes exactly these two fatal deviations.

Acknowledgments

This work began in 2023, and the final writeup is a collaboration between human and artificial intelligence. Human intelligence was solely responsible for all the conceptual

contributions, and for devising the main AMM adaptive clinching mechanism. AI proved our conjecture regarding Sybil-robust incentive compatibility.

Elaine Shi acknowledges Hubert Chan and Alireza Farhadi for helpful technical discussions during an earlier phase of the project. Elaine Shi is also grateful to Leo Fan and his family for their kindness, generosity, and the logistical support that made this cross-institutional collaboration possible.

References

[ABEP11] Haris Aziz, Yoram Bachrach, Edith Elkind, and Mike Paterson. False-name manipulations in weighted voting games. *Journal of Artificial Intelligence Research*, 40:57–93, 2011.

[AER25] Ittai Abraham, Yuval Efron, and Ling Ren. The latency cost of censorship resistance. *IACR Cryptol. ePrint Arch.*, 2025:2136, 2025.

[BCLL22] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente. Maximizing extractable value from automated market makers. In *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*, page 3–19, Berlin, Heidelberg, 2022.

[BCMX10] Sayan Bhattacharya, Vincent Conitzer, Kamesh Munagala, and Lirong Xia. Incentive compatible budget elicitation in multi-unit auctions. In *SODA*, pages 554–572, 2010.

[CBHLS12] Riccardo Colini-Baldeschi, Monika Henzinger, Stefano Leonardi, and Martin Starnberger. On multiple keyword sponsored search auctions with budgets. In *Proceedings of the 39th International Colloquium on Automata, Languages, and Programming (ICALP)*, volume 7392 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2012.

[CDLY22] Yukun Cheng, Xiaotie Deng, Yuhao Li, and Xiang Yan. Tight incentive analysis on sybil attacks to market equilibrium of resource exchange over general networks. In *Proceedings of the 23rd ACM Conference on Economics and Computation (EC)*, pages 792–793, 2022.

[CF23] Andrea Canidio and Robin Fritsch. Batching trades on automated market makers. In *AFT*, 2023.

[CF24] Andrea Canidio and Robin Fritsch. Arbitrageurs' profits, lvr, and sandwich attacks: batch trading as an amm design response. 2024.

[CH24] Andrea Canidio and Felix Henneke. Fair combinatorial auction for blockchain trade intents: Being fair without knowing what is fair, 2024.

[Con08] Vincent Conitzer. Anonymity-proof voting rules. In *Internet and Network Economics (WINE)*, pages 295–306, 2008.

[cow] https://cow.fi/cow-protocol.

[CWS25] T-H. Hubert Chan, Ke Wu, and Elaine Shi. Mechanism design for automated market makers. In *AFT*, 2025.

[dec] Challenging periods reimagined: The key role of sequencer decentralization. Ethereum Research.

[DHH13] Nikhil R. Devanur, Bach Q. Ha, and Jason D. Hartline. Prior-free auctions for budgeted agents. In *Proceedings of the 14th ACM Conference on Electronic Commerce (EC)*, pages 287–304, 2013.

[DHS12] Paul Dütting, Monika Henzinger, and Martin Starnberger. Auctions with heterogeneous items and budget limits. In *Proceedings of the 8th International Conference on Web and Internet Economics (WINE)*, volume 7695 of *Lecture Notes in Computer Science*, pages 44–57. Springer, 2012.

[DLN08] Shahar Dobzinski, Ron Lavi, and Noam Nisan. Multi-unit auctions with budget limits. In *Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '08, pages 260–269, USA, 2008. IEEE Computer Society.

[DP14] Shahar Dobzinski and Renato Paes Leme. Efficiency guarantees in auctions with budgets. In *Proceedings of the 41st International Colloquium on Automata, Languages, and Programming (ICALP)*, volume 8572 of *Lecture Notes in Computer Science*, pages 392–404. Springer, 2014.

[FLSS11] Amos Fiat, Stefano Leonardi, Jared Saia, and Piotr Sankowski. Single valued combinatorial auctions with budgets. In *Proceedings of the 12th ACM Conference on Electronic Commerce (EC)*, pages 223–232, 2011.

[foc] Eip-7805: Fork-choice enforced inclusion lists (focil). `https://eips.ethereum.org/EIPS/eip-7805`.

[FP23] Matheus Venturyne Xavier Ferreira and David C. Parkes. Credible decentralized exchange design via verifiable sequencing rules. In *STOC*, 2023.

[GLT20] Yotam Gafni, Ron Lavi, and Moshe Tennenholtz. VCG under sybil (false-name) attacks – A Bayesian analysis. In *Proceedings of the AAAI Conference on Artificial Intelligence*, pages 1966–1973. AAAI Press, 2020.

[GMP12] Gagan Goel, Vahab Mirrokni, and Renato Paes Leme. Polyhedral clinching auctions and the AdWords polytope. In *STOC*, 2012.

[GMP13] Gagan Goel, Vahab Mirrokni, and Renato Paes Leme. Clinching auctions with online supply. In *SODA*, pages 605–619, 2013.

[GMP14] Gagan Goel, Vahab Mirrokni, and Renato Paes Leme. Clinching auctions beyond hard budget constraints. In *Proceedings of the 15th ACM Conference on Economics and Computation (EC)*, pages 167–184, 2014.

[GNR25] Pranav Garimidi, Joachim Neu, and Max Resnick. Multiple concurrent proposers: Why and how. Cryptology ePrint Archive, Paper 2025/1772, 2025.

[HS22] Hiroshi Hirai and Ryosuke Sato. Polyhedral clinching auctions for two-sided markets. *Mathematics of Operations Research*, 47(1):259–285, 2022.

[ICO+10] Atsushi Iwasaki, Vincent Conitzer, Yoshifusa Omori, Yuko Sakurai, Taiki Todo, Mingyu Guo, and Makoto Yokoo. Worst-case efficiency ratio in false-name-proof combinatorial auction mechanisms. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 633–640, 2010.

[IYT03] Atsushi Iwasaki, Makoto Yokoo, and Kenji Terada. A robust open ascending-price multi-unit auction protocol against false-name bids. In *Proceedings of the 4th ACM Conference on Electronic Commerce (EC)*, pages 85–92, 2003.

[KDC22] Kshitij Kulkarni, Theo Diamandis, and Tarun Chitra. Towards a theory of maximal extractable value I: constant function market makers. *CoRR*, abs/2207.11835, 2022.

[KDK22] Mahimna Kelkar, Soubhik Deb, and Sreeram Kannan. Order-fair consensus in the permissionless setting. In *APKC '22: Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop*, 2022.

[KDL+23] Mahimna Kelkar, Soubhik Deb, Sishan Long, Ari Juels, and Sreeram Kannan. Themis: Fast, strong order-fairness in Byzantine consensus. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 475–489. Association for Computing Machinery, 2023.

[Kur20] Klaus Kursawe. Wendy, the good little fairness widget: Achieving order fairness for blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020.

[KZGJ20] Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels. Order-fairness for byzantine consensus. In *CRYPTO*, page 451–480, 2020.

[LM12] Ron Lavi and Marina May. A note on the incompatibility of strategy-proofness and Pareto-optimality in quasi-linear settings with public budgets. *Economics Letters*, 115(1):100–103, 2012.

[LSZ26] Yuhao Li, Elaine Shi, and Mengqian Zhang. A trilemma in amm mechanism design. In *Financial Cryptography and Data Security (FC)*, 2026.

[LX15] Pinyan Lu and Tao Xiao. Improved efficiency guarantees in auctions with budgets. In *Proceedings of the 16th ACM Conference on Economics and Computation (EC)*, pages 397–413, 2015.

[MMR24] Jason Milionis, Ciamac C. Moallemi, and Tim Roughgarden. A Myersonian framework for optimal liquidity provision in automated market makers. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 81:1–81:19. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024.

[Mye81] Roger B. Myerson. Optimal auction design. *Math. Oper. Res.*, 6(1), 1981.

[Par23] Andreas Park. The conceptual flaws of decentralized automated market making. *Management Science*, 69(11):6731–6751, 2023.

[QZLG21] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. Attacking the DeFi ecosystem with flash loans for fun and profit. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I*, 2021.

[RGGM24] Geoffrey Ramseyer, Mohak Goyal, Ashish Goel, and David Mazières. Augmenting batch exchanges with constant function market makers. In *EC*, 2024.

[SSIY08] Yuko Sakurai, Yasumasa Saito, Atsushi Iwasaki, and Makoto Yokoo. Beyond quasi-linear utility: Strategy/false-name-proof multi-unit auction protocols. In *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, volume 2, pages 417–423, 2008.

[SYM99] Yuko Sakurai, Makoto Yokoo, and Shigeo Matsubara. A limitation of the generalized Vickrey auction in electronic commerce: Robustness against false-name bids. In *AAAI*, 1999.

[SZCL26] Elaine Shi, Mengqian Zhang, Hao Chung, and Yuhao Li. Otter: A provably mev-resilient automated market maker via surplus redistribution. arXiv:2609.03474, 2026.

[Uni] Uniswap. https://app.uniswap.org/.

[VK23] Mohammad Amin Vafadar and Majid Khabbazian. Condorcet attack against fair transaction ordering. In *5th Conference on Advances in Financial Technologies (AFT 2023)*, volume 282 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 15:1–15:21. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2023.

[YNZ25] Sen Yang, Kartik Nayak, and Fan Zhang. Decentralization of ethereum's builder market. In *2025 IEEE Symposium on Security and Privacy (SP)*, page 1512–1530. IEEE, May 2025.

[YSM01] Makoto Yokoo, Yuko Sakurai, and Shigeo Matsubara. Robust combinatorial auction protocol against false-name bids. *Artificial Intelligence*, 130(2):167–181, 2001.

[YSM04] Makoto Yokoo, Yuko Sakurai, and Shigeo Matsubara. The effect of false-name bids in combinatorial auctions: New fraud in Internet auctions. *Games and Economic Behavior*, 46(1):174–188, 2004.

[ZQT+21] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc Viet Le, and Arthur Gervais. High-frequency trading on decentralized on-chain exchanges. In *IEEE Symposium on Security and Privacy*, 2021.

[ZSC+20] Yunhao Zhang, Srinath Setty, Qi Chen, Lidong Zhou, and Lorenzo Alvisi. Byzantine ordered consensus without byzantine oligarchy. In *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)*, 2020.

[ZXS+26] Chengkai Zhang, Lirong Xia, Elaine Shi, Mengqian Zhang, Qishen Han, and Yuhao Li. Tight characterizations of amm mechanism design under weak efficiency. Manuscript, 2026.

A Fixed and Online Supply as Constant Targets

The target-based clinching mechanism of Section 4.1 separates the clinching mechanics from the source of supply. This appendix shows that the two classical supply models are instances of it: the ordinary adaptive clinching auction [DLN08, BCMX10] for a fixed divisible supply, and adaptive clinching with exogenous online supply, due to Goel, Mirrokni, and Paes Leme [GMP13]. In both cases the target ignores the auction state (X, Y) and the clock price: it is the constant function equal to the available supply. The admissibility requirements of Definition 4.2 then hold trivially.

The main content of the appendix is a rule-by-rule correspondence showing that, with a constant target, the rules of Section 3 reduce to those of the classical auction. The only genuine boundary convention is that the abstract clock starts at a positive price $p_\star$, whereas the classical clock starts at zero. A constant target also attains its capacity, but the zero-trade completion convention makes that boundary identical to the classical clock after all supply has been allocated and creates no exception in the incentive theorem.

A.1 Fixed Divisible Supply

The classical auction. We recall the adaptive clinching auction in the notation of Section 3. A divisible supply $s > 0$ of a single good is offered to finitely many identities; [BCMX10] normalizes $s = 1$, whereas [GMP13] keeps s general. Identity i reports a value $v_i \geq 0$ per unit and a hard budget $q_i \geq 0$; these are v_i and B_i in [BCMX10, GMP13]. A price clock p ascends from zero. At clock price p, identity i has cumulative allocation x_i, cumulative payment y_i, and effective remaining budget b_i, which equals $q_i - y_i$ while the identity is in the auction and is set to zero when it exits. The unallocated supply is $S = s - \sum_i x_i$, the demand of identity i is b_i/p, and the sets Active, Exit, and Clinch are those of (12) and (14). The auction maintains the supply invariant (13). Every trade is charged at the current clock price. A clinching identity trades at the rates

$$\frac{\mathrm{d}x_i}{\mathrm{d}p} = \frac{S}{p}, \qquad \frac{\mathrm{d}y_i}{\mathrm{d}p} = S, \qquad \frac{\mathrm{d}b_i}{\mathrm{d}p} = -S, \qquad i \in \mathsf{Clinch}, \tag{79}$$

and no other identity trades [BCMX10, Figure 1, Step (II)], [GMP13, Definition 4.2(ii)]. When the clock reaches the value of one or more identities, the stopping condition (20) is tested. If it holds, every active identity receives its full demand b_i/p, the exiting identities receive the rest of the supply, and the auction ends [BCMX10, Figure 1, Step (I)].

Otherwise the exiting budgets are cancelled, and each active identity i clinches

$$\left(S - \sum_{k \in \mathsf{Active} \setminus \{i\}} \frac{b_k}{p}\right)_+ \tag{80}$$

units at the exit price [BCMX10, Lemma 3.1], [GMP13, Definition 4.2(iv)].

Definition A.1 (Constant target)**.** Fix a supply $s > 0$ and an initial price $p_\star > 0$. The *constant target* is

$$T_s^{\mathrm{fix}}(p, X, Y) := s \qquad \text{for every } (p, X, Y) \in \mathcal{D}_s^{\mathrm{fix}},$$

on the state domain

$$\mathcal{D}_s^{\mathrm{fix}} := \{(p, X, Y) : p \geq p_\star,\ 0 \leq X \leq s,\ Y \geq 0\},$$

Let σ^{fix} denote the trivial environment description, and define the constant-target specification

$$\mathfrak{T}_s^{\mathrm{fix}} := (p_\star, \sigma^{\mathrm{fix}}, T_s^{\mathrm{fix}}, \mathcal{D}_s^{\mathrm{fix}}, s).$$

Its residual supply $S = s - X$ is the unallocated supply of the classical auction. For the unit supply of [BCMX10], the target is the constant 1.

Proposition A.2 (Admissibility of the constant-target specification)**.** *For every $s > 0$ and $p_\star > 0$, $\mathfrak{T}_s^{\mathrm{fix}}$ is an admissible abstract target-based mechanism. Its frozen-state clock rate vanishes, $\lambda \equiv 0$, and its only supply lump is the initial release $T_s^{\mathrm{fix}}(p_\star, 0, 0) = s$. Unlike the AMM capacity, the capacity s is attainable: $T_s^{\mathrm{fix}} = X$ precisely when $X = s$.*

Proof. We verify the five requirements of Definition 4.2 in order.

- *Feasibility and partition independence.* On the domain, $X \leq s = T_s^{\mathrm{fix}} = \overline{X}$. A constant depends on the bidders through nothing at all; in particular it depends neither on their names nor on the partition of a budget among identities.
- *Fixed-price invariance.* If $0 \leq \delta \leq S = s - X$, then $X + \delta \leq s$ and $Y + p\delta \geq 0$, so the updated state lies in $\mathcal{D}_s^{\mathrm{fix}}$. The target is unchanged because it is constant.
- *Target decreases with mark-to-market gain.* Both targets in (26) equal s. The implication therefore holds, with equality, whatever the two gains are.
- *Clock regularity.* For fixed (X, Y), the map $p \mapsto s$ is constant. It is nondecreasing, right-continuous, of bounded variation, free of jumps, and absolutely continuous, and (27) gives $\lambda = 0$.
- *Eventual supply release.* The target equals X only if $X = s = \overline{X}$. Thus there is no state satisfying the premise $T_s^{\mathrm{fix}} = X < \overline{X}$ of (28).

Finally, $\mathcal{D}_s^{\mathrm{fix}}$ contains the initial state $(p_\star, 0, 0)$ and is closed under raising p with (X, Y) held fixed. The positive initial target is released at $p_\star$ as the initial lump, as prescribed after (10). □

Proposition A.3 (The constant-target mechanism is adaptive clinching)**.** *The target-based clinching mechanism associated with $\mathfrak{T}_s^{\mathrm{fix}}$ is the adaptive clinching auction for supply s with its clock started at $p_\star$. Equivalently, apply the target substitution (29) with $(p_\star, T_\sigma, \overline{X}_\sigma) = (p_\star, T_s^{\mathrm{fix}}, s)$. More precisely:*

1. Start. *Identities with $v_i < p_\star$ are ineligible. The whole supply is released at $p_\star$ as the initial lump, so $S = s$, and the event rules in items 3 and 4 are applied at $p_\star$, with the identities having $v_i = p_\star$ as the exiting identities.*

2. Continuous evolution. *The derived rate (30) is $\gamma = S$. Clinching identities trade at the classical rates (79), no other identity trades, and, with $c = |\mathsf{Clinch}|$,*

$$\frac{\mathrm{d}S}{\mathrm{d}p} = -\frac{cS}{p}, \qquad \frac{\mathrm{d}h}{\mathrm{d}p} = -S. \tag{81}$$

   In particular, S remains positive between events.

3. Nonstopping exits. *If the stopping test fails, the one-shot restoration purchase (24) of an active identity i is the classical clinch (80).*

4. Stopping. *The stopping test (20) and the full-demand purchases of the active identities are Step (I) of [BCMX10, Figure 1], and the proportional rule (22) specifies how the remainder L of (21) is divided among the exiting identities. At every stopping price above $p_\star$, some identity exits and*

$$0 \le L \le \frac{1}{p}\Big(B_E - \max_{i \in \mathsf{Exit}} b_i\Big). \tag{82}$$

   Thus $L = 0$ unless at least two identities exit simultaneously, the exiting identities can afford all of L, and the stopping allocation sells the entire residual supply.

5. Capacity completion and termination. *After the initial release the target has no lump. A nonstopping event saturates capacity exactly when it leaves a single active identity, which buys the entire residual supply at that price. The allocation and payment are then complete, and the clock follows the zero-trade tail of Lemma 4.5 until that identity exits. Every run that does not enter such a tail ends with a stopping allocation. In particular, before capacity saturation at least two identities are active whenever a run continues.*

Proof. Item 1 is the initialization rule stated after (10), together with the eligibility rule that accompanies (29).

For item 2, Proposition A.2 gives $\lambda = 0$, so Lemma 4.4 yields $\gamma = S + p\lambda = S$. Equations (31) and (32) then become (79), and (33) becomes (81). On an event-free interval beginning at p_a, the first equation integrates to $S(p) = S(p_a)(p_a/p)^c$, which is positive whenever $S(p_a)$ is.

For item 3, after the cancellation (23) the aggregate budget is $B = \sum_{k \in \mathsf{Active}} b_k$. Hence $h^\star = \sum_{k \in \mathsf{Active}} b_k - pS$ and

$$\frac{b_i - h^\star}{p} = S - \sum_{k \in \mathsf{Active} \setminus \{i\}} \frac{b_k}{p}. \tag{83}$$

The purchase (24) is made exactly when this quantity is positive, which is (80).

For item 4, the test and the purchases $\mathrm{Buy}(i, b_i/p; p)$ are literally Step (I) of [BCMX10, Figure 1]. Let $p > p_\star$ be a stopping price. Some identity exits at p. Indeed, by Lemma 4.7 the stopping test is equivalent to $B_E \ge h$. If an identity i is still active at p, then $h \ge b_i > 0$ by (15), so $B_E > 0$; if none is, the identities that

were active immediately before p all exit at p. Every $i \in \mathsf{Exit}$ was active immediately before p, and a constant target has no lump at p. The supply invariant therefore gives

$$S \le D_{-i} = \sum_{k \in \mathsf{Active}} \frac{b_k}{p} + \sum_{k \in \mathsf{Exit} \setminus \{i\}} \frac{b_k}{p}.$$

Subtracting the active demand yields $L \le (B_E - b_i)/p$ for every $i \in \mathsf{Exit}$, which is (82); and $L \ge 0$ is the stopping test. Consequently $L \le B_E/p$, the proportional rule distributes exactly L, and the total stopping allocation is $\sum_{k \in \mathsf{Active}} b_k/p + L = S$.

For item 5, a lump is an upward jump of the target, and a constant has none after its initial release. By item 2, S does not vanish between events, so $S = 0$ can only be produced by the fixed-price purchases of an event. A stopping event ends the run. At a nonstopping event, let m be the number of active identities with $b_i > h^\star$. If $m = 0$, nothing is bought and S stays positive. If $m \ge 1$, then $pS = \sum_{k \in \mathsf{Active}} b_k - h^\star$ shows that the restoration purchases leave the residual supply

$$S - \sum_{i \in \mathsf{Active}} \frac{(b_i - h^\star)_+}{p} = \frac{1}{p}\Big(\sum_{i \in \mathsf{Active}:\, b_i \le h^\star} b_i + (m-1)h^\star \Big).$$

Since $h^\star > 0$ by Lemma 4.7 and active budgets are positive, this vanishes if and only if Active is a singleton. Conversely, a single active identity i at a nonstopping event has $b_i > b_i - pS = h^\star$ and buys S by (83). Then $S = 0$ and $X = s$, so the capacity is saturated and Lemma 4.5 applies. An event that leaves no active identity passes the stopping test trivially. Hence, outside the zero-trade tail, at least two identities are active whenever a run continues. □

The zero-trade completion in item 5 is exactly the classical convention: once the supply has been exhausted, the clock keeps rising with $S = 0$ until the surviving identity reaches its value, and nothing further is traded. Apart from the start price, the only difference between the two descriptions is the treatment of identities that exit simultaneously. [BCMX10, GMP13] process them one at a time in a fixed order. At a nonstopping event this produces the same state as the simultaneous cancellation and one-shot restoration, as noted after (24). At a stopping event it divides L among the tied exiting identities in an order-dependent way, where the mechanism of Section 3 uses the proportional rule. By item 4 of Proposition A.3, the two agree whenever no two identities exit at the stopping price.

The remaining difference is the start of the clock. The classical clock starts at zero, where every positive budget has infinite demand, whereas Section 4.1 fixes $p_\star > 0$. By the *zero-start auction* we mean the auction of items 2–5 above with the clock started at zero and identities with $v_i = 0$ removed at the outset. If a single identity of positive value and budget remains, no other identity has demand, and (80) lets it clinch the whole supply at price zero.

Lemma A.4 (Starting the clock at zero)**.** *Consider a profile in which the set P of identities with $v_i > 0$ and $q_i > 0$ has at least two elements, and put*

$$p^\dagger := \min\Big\{ \min_{i \in P} v_i,\ \frac{1}{s}\Big(\sum_{i \in P} q_i - \max_{i \in P} q_i \Big) \Big\} > 0. \tag{84}$$

For every $p_\star \in (0, p^\dagger)$, the zero-start auction and the target-based mechanism for $(p_\star, T_s^{\mathrm{fix}}, s)$ produce the same outcome.

Proof. The price $p^\dagger$ is the first event of the zero-start auction [GMP13, proof of Theorem D.2]. Indeed, no identity of P exits below $\min_{i\in P} v_i$, and as long as nothing has been traded,

$$D_{-i} = \sum_{j\in P\setminus\{i\}} \frac{q_j}{p} \geq \frac{1}{p}\Big(\sum_{j\in P} q_j - \max_{j\in P} q_j\Big) > s = S \qquad \text{for } p < p^\dagger,$$

so the supply invariant is strict and nobody clinches. At price $p_\star < p^\dagger$ the state of the zero-start auction is therefore $x_i = y_i = 0$, $b_i = q_i$ for $i \in P$, and $S = s$.

This is also the state of the target-based mechanism after its initial event. Identities outside P are ineligible or have no budget. No identity of P has $v_i = p_\star$, so none exits. The stopping test fails because $\sum_{i\in P} q_i > p_\star s$. After the initial release, $h^\star = \sum_{i\in P} q_i - p_\star s > \max_{i\in P} q_i$, so no restoration purchase is made. From $p_\star$ on, both auctions follow the rules of Proposition A.3. □

Thus $p_\star$ acts as a reserve price, and the classical auction is recovered for all sufficiently small $p_\star$: profile by profile, and simultaneously on any finite family of profiles, such as a merged profile and a Sybil profile. The start price is visible only on a profile with a single identity of positive value and budget. That identity receives $\min\{s, q_i/p_\star\}$ units at the unit price $p_\star$, which tends to the whole supply at zero payment as $p_\star \downarrow 0$.

A.2 Exogenous Online Supply

In the online supply model of [GMP13, Definition 3.1 and Example 3.2], the supply of the good is revealed over steps $t = 0, 1, \ldots, m$ as a nondecreasing sequence of cumulative supplies

$$0 = s_0 \leq s_1 \leq \cdots \leq s_m. \tag{85}$$

The sequence is exogenous: it may be deterministic, random, or adversarial, but it does not depend on the reports, and at step t the auctioneer knows only $s_0, \ldots, s_t$. The identities, their reports, and their budgets are fixed before the first step. At every step the auctioneer must announce a cumulative allocation and a cumulative payment for each identity, and it may only augment those of the previous step. *Online adaptive clinching* announces, at step t, the outcome $(x(s_t), y(s_t))$ of the adaptive clinching auction of Appendix A.1 run to completion with supply s_t. Between steps $t-1$ and t it therefore allocates $x(s_t) - x(s_{t-1})$ and charges $y(s_t) - y(s_{t-1})$.

Let the environment description be the supply revealed so far, and let the target be its last entry:

$$\sigma_t := (s_0, \ldots, s_t), \qquad T_{\sigma_t}(p, X, Y) := s_t, \qquad \overline{X}_{\sigma_t} := s_t, \qquad \mathcal{D}_{\sigma_t} := \mathcal{D}^{\mathrm{fix}}_{s_t},$$
$$\mathfrak{T}_t := (p_\star, \sigma_t, T_{\sigma_t}, \mathcal{D}_{\sigma_t}, \overline{X}_{\sigma_t}).$$

Proposition A.5 (Online supply as a family of constant targets)**.** *Fix a realized supply path (85) and a step t with $s_t > 0$. Then $\mathfrak{T}_t$ is an admissible abstract target-based mechanism, and the cumulative outcome of online adaptive clinching after step t, with every clock started at $p_\star$, is the outcome of its target-based clinching mechanism. The description σ_t is common to all bid profiles. If $s_t = 0$, no supply has arrived and the cumulative outcome is zero.*

Proof. Since $T_{\sigma_t} = T^{\mathrm{fix}}_{s_t}$, the first two claims are Propositions A.2 and A.3, with Lemma A.4 relating the start price $p_\star$ to a clock started at zero. During the run that settles step t, the fixed environment description is σ_t: the step index is not the clock. Clock regularity therefore holds with $\lambda_{\sigma_t} = 0$ and no target lump. Finally, σ_t is determined by the supply path alone. Because the path is exogenous, every bid profile faces the same σ_t, and hence the same target and the same capacity. This is what Definition 4.2 requires of the capacity, and what Section 4.6 requires when it lets the merged run and the Sybil run share the same environment description. □

Remark A.6 (Two time axes). The online step t and the clock price p are different objects. At step t the clock is run afresh from $p_\star$ against the constant target s_t; the auction does not pause one ascending clock and resume it when more supply arrives. Accordingly, online adaptive clinching is a family of target-based mechanisms indexed by σ_t, one for every prefix of the supply path, and not a single run with a growing target. A statement about one prefix, such as a single-run lemma of Section 4.4 or a comparison between two bid profiles that face the same σ_t, is a statement about one admissible abstract target-based mechanism. Whether the increments $x(s_t) - x(s_{t-1})$ and $y(s_t) - y(s_{t-1})$ are nonnegative, so that the family can be implemented online, is a different kind of statement: it compares the targets $T_{\sigma_{t-1}}$ and T_{σ_t} on one fixed bid profile. This is the supply-monotonicity theorem [GMP13, Theorem 4.1]. It is neither used nor implied by the results of Section 4. On a profile that has at least two identities of positive value and budget and no tied values, and with $p_\star$ below the threshold (84) for the largest supply s_m, which is the smallest threshold along the path, every run is exactly the auction of [GMP13], and that theorem applies verbatim.

Remark A.7 (A different notion: supply released along the clock). Definition 4.2 also allows the fixed environment description to contain a schedule indexed by the clock. The simplest example is an exogenous release schedule: a nondecreasing, right-continuous function $s\colon [p_\star, \infty) \to [0, \infty)$, not identically zero, whose continuous part is locally absolutely continuous, together with

$$\sigma := s(\cdot), \qquad T_\sigma(p, X, Y) := s(p), \qquad \overline{X}_\sigma := \sup_p s(p),$$
$$\mathcal{D}_\sigma := \{(p, X, Y) : p \geq p_\star,\ 0 \leq X \leq s(p),\ Y \geq 0\}.$$

The first three requirements hold because the target ignores (X, Y), and the domain is closed under raising the clock because s is nondecreasing. Clock regularity is the assumption on s, with $\lambda_\sigma = s'(p)$ almost everywhere and with supply lumps at the jumps of s. If $s(p) = X < \sup_q s(q)$, then some $p' > p$ satisfies $s(p') > X$, which verifies (28). Here a single clock is never restarted: supply that arrives at clock price p is sold at prices at least p, clinchers trade at the rate $\gamma = S + ps'(p)$ of (30), and the mechanism waits while $s(p) = X$. This variant exercises the clauses of Definition 4.2 that concern clock-dependent environment data, target lumps, and waiting on $T_\sigma = X$, none of which is used by the AMM target or by a constant target. It is not the model of [GMP13], in which every prefix is settled by a fresh run, and we mention it only to illustrate the definition.

A.3 Incentives for Fixed and Online Supply

The general incentive theorem now applies directly at an attained capacity: capacity saturation begins a zero-trade tail rather than ending the execution with unused budgets. Thus no separate terminal comparison is needed.

Corollary A.8 (Fixed- and online-supply incentives)**.** *Let $s > 0$ and $p_\star > 0$. In the target-based mechanism for the constant target T_s^{fix}, truthful participation as the merged identity (V, Q), where $V \geq p_\star$, weakly dominates every same-direction Sybil strategy (43). Hence, at every step t with $s_t > 0$ of an exogenous online supply path, the truthful merged identity weakly dominates every such strategy in cumulative utility. The same conclusions hold for the classical zero-start auctions, with the simultaneous proportional rule at tied stopping exits.*

Proof. The constant-target specification is admissible by Proposition A.2, so the fixed-supply conclusion is an immediate application of Theorem 4.18. At online step t, Proposition A.5 identifies the cumulative outcome with the same mechanism for the constant target $T_{\sigma_t} = T_{s_t}^{\mathrm{fix}}$. The supply prefix σ_t is exogenous and therefore common to the merged and Sybil runs, so the theorem applies pointwise to that prefix.

For the zero-start conclusions, assume $V > 0$ and $Q > 0$, since otherwise no strategy yields positive utility. If the merged profile and the Sybil profile each contain at least two identities of positive value and budget, choose $p_\star$ below V and below both thresholds (84); on a finite online path it may be chosen below the thresholds for the largest supply, and hence for every prefix. By Lemma A.4, the two positive-start executions equal their zero-start counterparts. In the remaining singleton cases the comparison is immediate: either no outsider has positive value and budget, and the merged identity obtains the whole supply at zero payment, or the Sybil group has no such identity and obtains nothing. □