Efficient Order-Preserving Redistribution of Troves

November 2020

Contents

1 Introduction

The Liquity protocol [1] issues a USD-pegged stablecoin LUSD that is redeemable at face value against ETH: any owner of LUSD can exchange their stablecoins for equivalent value in the underlying collateral at any time. The ETH paid to the redeemer is taken from the borrowers' collateralized debt positions ("troves") in ascending order of collateral ratio. In other words, the system uses the redeemed LUSD to repay the debt on the riskiest trove with the currently lowest individual collateral ratio (ICR), and transfers a corresponding amount of ETH from the trove to the redeemer. If the redeemed LUSD is larger than the debt on the riskiest trove, the system proceeds with the second riskiest trove, and so on.

To allow for efficient redemptions despite Ethereum's gas constraints, the system keeps troves ordered by ICR, so that it can iterate over the linked list starting from the bottom. It is not feasible to sort the list after every operation.

Troves with an insufficient ICR are subject to liquidation. Given that Liquity's fallback liquidation mechanism [1] redistributes the collateral and debt of a liquidated trove between all remaining active troves, it must be ensured that redistributions do not break trove ordering.

Redistribution in proportion to the collateral size of active troves maintains ordering, as can be easily shown (see 8 Appendix). However, in practice, it is clear that redistributing in a "push" based manner - iterating over all troves and updating their collateral and debt - does not scale, and has

computational complexity of $O(n)$, where n is the number of troves.

Previous work by Batog et al [2] derived a scalable $O(1)$ method to assign proportional rewards to a large number of recipients, as long as the basis for their rewards ("stakes") do not change over time. The method is "pull" based: instead of adjusting all recipient positions upon every reward event, the update is deferred to the moment at which an owner changes their position. In the described approach rewards are stored separately from the initial stakes, and do not compound. That is to say, past accumulated rewards are not included in future reward calculations.

It turns out that this approach thus cannot be applied to Liquity as is. As the system undergoes reward events, a given trove's ratio of initial collateral to its total collateral shrinks. Rewards are based on a smaller and smaller share of the total collateral. This is fine, as long as all active troves have experienced all reward events - in this case, ordering is maintained since all troves are affected by the same change.

However, a problem arises when a new trove is created after active troves have received reward shares. Such "fresh" troves (with no accumulated rewards) would thus gain an advantage in redistributions over older troves whose stakes may be smaller than their actual collateral due to the liquidations that have taken place in the meantime. In other words, a "fresh" trove that has experienced fewer rewards than the earlier troves would receive a disproportionate share of subsequent rewards relative to its collateral. Though, a trove's collateral ratio must always be based on its entire collateral, which does include accumulated rewards.

This discrepancy means that the reward distribution scheme described in [2] can break the ordering of troves by collateral ratio. To remedy this, we modify the original approach by introducing a "corrected stake", to ensure fresh troves do not receive disproportionate rewards. We then show that this corrected stake preserves trove ordering.

2   Troves and Liquidations

Troves are collateralized debt positions held by individual borrowers, defined by their amount of debt d (in LUSD) and collateral c (in ETH).

Let γ_i denote the individual collateral ratio (ICR) of a trove i, i.e. the ratio of its collateral to its debt:

$$\gamma_i = \frac{c_i}{d_i} \tag{1}$$

If γ_i falls below a minimum threshold δ, the trove is subject to liquidation. As long as there are sufficient LUSD tokens in the Stability Pool, the system can use them to repay the liquidated debt.

If the Stability Pool is empty, the trove's collateral and debt are redistributed to all active troves in the system as part of the liquidation process (a trove is called *active* as long as it has not been liquidated or closed by their owner). Every existing borrower with an open trove thus receives a share of both the collateral and the debt of the liquidated trove.

Collateral and debt shares from liquidations are proportional to the *entire* collateral of the recipient troves, i.e. taking into account accumulated "rewards" from prior liquidations. Thus, in the event of a redistribution of a trove k, an active trove i receives the following collateral and debt shares x_i, y_i:

$$(x_i, y_i) = \left(\frac{c_i}{C} \cdot c_k, \frac{c_i}{C} \cdot d_k \right) \tag{2}$$

where $C = \sum c_j$ is the total collateral in the system.

The rewards compound across multiple redistribution events.

3 Trove Ordering

To ensure that the troves can be reliably accessed using a linked list, it is crucial to maintain the ordering of the troves (by ICR) throughout all redistribution events E_k.

The ordering is maintained if $\forall E_k, i, j : (\gamma_i > \gamma_j \implies \gamma_i' > \gamma_j')$, where γ_i' and γ_j' is the ICR of troves i and j after E_k.

It is easy to prove that a redistribution in proportion to the collateral of the recipient trove as described by equation 2 troves maintains ordering. See 8 Appendix.

4 Efficient Reward Distribution

4.1 Scalable Reward Distribution with Fixed Stakes

A naive "push" based implementation of the redistribution ("strawman approach"), where rewards don't compound, would iterate over all participants and compute the debt and collateral shares for each recipient i separately whenever the system distributes such rewards. Thus, at a reward event t, every recipient would receive the following reward share:

$$r_{i,t} = s_i \cdot \frac{R_t}{S_t} \tag{3}$$

where R_t is the reward distributed at t, $r_{i,t}$ the reward share of recipient i, s_i the stake of recipient i, and S_t the sum of the stakes of all recipients, i.e. $\sum s_j$.

Note that s_i does not depend on t, and is thus fixed throughout multiple reward events. The sum of s_i may vary over time because the set of them may change, stakes entering or leaving the set, but each amount s_i is fixed while it's in the set.

Based on this prerequisite, [2] suggests a scalable $O(1)$ method of distributing such rewards by deferring the reward computation. The total reward share of i from all reward events that occur between time t_1 and t_2 can be written as a sum of its reward shares with the (fixed) stake s_i being factored out:

$$\sum_{t=t_1+1}^{t_2} r_{i,t} = s_i \cdot \sum_{t=t_1+1}^{t_2} \frac{R_t}{S_t} \tag{4}$$

Let Q_t denote the sum of all rewards per total staked amount up to instant t:

$$Q_t = \sum_{k=0}^{t} \frac{R_t}{S_t} \tag{5}$$

Assuming stake s_i is deposited at moment t_1 and then withdrawn at moment $t_2 > t_1$, we can use the sum Q_t to compute the total reward share for participant i since

$$r_i = s_i \cdot \sum_{t=t_1+1}^{t_2} \frac{R_t}{S_t} \tag{6}$$

can be written as

$$r_i = s_i \cdot (Q_{t_2} - Q_{t_1}) \tag{7}$$

As Q_t is monotonic, we can simply track the current (latest) value of Q as a running sum, and snapshot it whenever we expect it to be required for a later computation, i.e. whenever a participant changes their stake.

To compute the total (accumulated) reward for participant i, we can then use following formula:

$$r_i = s_i \cdot (Q - Q_{t_1}) \tag{8}$$

4.2 Corrected Stake Approach for Variable Stakes

In Liquity, collateral and debt shares from liquidations are proportional to the entire collateral of the recipient troves. The redistribution must cope with the fact that some fraction of a trove's entire collateral is the accumulated reward from prior liquidations, and this fraction varies across troves.

The "strawman" approach in 4.1, with rewards proportional to the initial stake, neglects this: it over-rewards fresh troves, and under-rewards older troves.

We introduce a corrected stake s_i to restore proportional reward distribution:

$$s_i = \begin{cases} c_i & for \ C_\emptyset = 0 \\ c_i \cdot \frac{S_\emptyset}{C_\emptyset} & for \ C_\emptyset > 0 \end{cases} \tag{9}$$

The corrected stake s_i is chosen such that it earns rewards from liquidations equivalent to a trove that would have accumulated c_i total collateral by the time the fresh trove i was created.

$S_\emptyset$ and $C_\emptyset$ are the respective snapshots of the total stakes and total collateral in the system, taken immediately after the last liquidation event. Note that with this terminology, the total collateral includes the total stakes, and therefore $C_\emptyset \geq S_\emptyset$

By extending the original formula from [2], we can thus express the collateral and debt share received by a trove by:

$$r_i = \begin{cases} c_i \cdot (Q - Q_{t_1}) & for \ C_\emptyset = 0 \\ c_i \cdot \frac{S_\emptyset}{C_\emptyset} \cdot (Q - Q_{t_1}) & for \ C_\emptyset > 0 \end{cases} \tag{10}$$

Note that r_i can stand for the collateral or the debt share of a recipient trove since both of them can be represented as "rewards" through R_t.

5 System Order Evolution

As mentioned above, we aim to prove that the corrected stake approach leaves the ordering of the troves by collateral ratio unchanged throughout all liquidations, regardless of any borrowers that change their troves' collateral between liquidation events.

Given that Liquity's fallback liquidation mechanism [1] redistributes the collateral and debt of a liquidated trove between all remaining active troves, it must be ensured that redistributions do not break trove ordering.

To break up the proof, we introduce the notion of *system order*.

Definition 5.1 (System Order). *A system of troves has an order, N. When the first trove is created, the system order equals 1.*

The order of a system remains constant throughout the following event sequence:

- *1 or more new troves are created*

- *1 or more troves are subsequently liquidated*

Definition 5.2 (System order evolution). *The first trove creation event after a series of liquidations triggers a system evolution, and the system order increases by 1.*

We capture the system order increase from order N to order $N+1$ in a system evolution function:

$$f(\Gamma_N) = \Gamma_{N+1} \tag{11}$$

Let Γ_1 define a system of troves with past liquidations, in which all active troves have received reward shares from all past liquidations. Γ_1 is a first-order system, and contains only stakes of first-order troves. Each first-order stake s_i is equal to it's collateral c_i, and $S = \sum s_i = \sum c_i$.

Let Γ_2 define an evolution of Γ_1, i.e. $\Gamma_2 = f(\Gamma_1)$. Γ_2 is a system with past liquidations, with $S = \sum s_i + \sum s_j$, where s_j is the stake of newly added troves j. Γ_2 is a second-order system, containing **both** *first-order* stakes $s_i = c_i$ which have experienced all liquidations, **and** *second-order* stakes s_j which have only experienced the liquidations after their creation.

In general, Γ_n is a system with n sequential pairs, each consisting of a trove creation period and a liquidation period. Troves created in a given trove creation period t have experienced only those liquidations that occurred in liquidation period t or greater.

5.1 At First-Order, Stake Equals Initial Collateral

For first-order systems, all troves were added before any liquidation events occurred. The snapshot $C_\emptyset$ is equal to 0. Therefore:

$$s_i = c_i \tag{12}$$

for all s_i, c_i in an Γ_1 system.

5.2 Intuition Behind Choice of Corrected Stake

The corrected stake effectively models the fresh trove's collateral c_i as a total collateral, which includes 'virtual' accumulated rewards. The corrected stake earns rewards for the trove as if the trove was first-order, and had been in the system from the beginning - thus maintaining proportional reward growth.
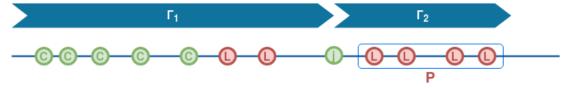
5.3 Outline of the Proof

We first prove that ICR equality is maintained with rewards proportional to corrected stakes - starting with the simplest case, and progressively generalizing, and finally we prove that order is maintained too.

- Lemma. We consider a system transition $\Gamma_1 \to \Gamma_2$ triggered by the creation of a trove j, followed by a liquidation of a trove k. For any trove i with $\gamma_i = \gamma_j$ in Γ_1, the corrected stake approach maintains $\gamma_i = \gamma_j$ in Γ_2.

- Lemma. We consider a system transition $\Gamma_1 \to \Gamma_2$ triggered by the creation of a trove j, followed by a set of liquidations P, such that $|P| > 1$ and $j \notin P$. For any trove i with $\gamma_i = \gamma_j$ in Γ_1, the corrected stake approach maintains $\gamma_i = \gamma_j$ in Γ_2.

- Lemma. We consider a system transition $\Gamma_1 \to \Gamma_2$ triggered by the creation of a trove j, followed by a set of creations N, and then by a set of liquidations P, such that $|N|, |P| > 0$ and $N \cap P = \emptyset$. For any trove i with $\gamma_i = \gamma_j$ in Γ_1, the corrected stake approach maintains $\gamma_i = \gamma_j$ in Γ_2.

- Theorem. In a second order system with M previous liquidations, and N second-order troves added after the last liquidation, ICR equality between a first-order trove and second-order trove holds across P subsequent liquidation events

- Lemma. For every 2nd order system Γ_2 there exists an equivalent first order system Γ_1 that contains only first-order stakes which have experienced all liquidations.

- Proposition. For every N^{th} order system Γ_N there exists an equivalent first order system Γ_1 that contains only first-order stakes which have experienced all liquidations.

- Corollary. In an nth order system with M previous liquidations, and N second-order troves added after the last liquidation, ICR equality between an $(n-1)^{th}$ order trove and n^{th} order trove holds across P liquidation events.

- Theorem. For every system Γ_N containing troves i and j with $\gamma_i > \gamma_j$ that transitions to Γ_{N+1}, the corrected stake approach maintains $\gamma_i > \gamma_j$.

6 Corrected Stake Approach Preserves Equality

Lemma 6.1. *Corrected Stake Preserves ICR Equality Across a Reward Event in a Second Order System with m Past Liquidations*

Proof. We consider the following event sequence:

- $n + m$ troves are created

- m troves are liquidated

- A fresh trove is created

- An old trove is liquidated

In other words, a first-order system of $n+m$ troves undergoes m trove liquidations, before evolving to second-order.

Consider the m past liquidations from the point of view of an active first-order $trove_i$. As per (9), the stake of $trove_i$ is $s_i = c_i$.

Let's define the reward from liquidating $trove_k$ received by $trove_i$ as the pair $R_i^k = (x_i^k, y_i^k)$ where x_i^k is the share of $trove_k$'s collateral received by $trove_i$ and y_i^k is the share $trove_k$'s debt absorbed by $trove_i$.

Let's call x_i the total accumulated collateral from rewards earned by $trove_i$. At the end of the first-order stage this is the sum of its collateral rewards from m past liquidations.

(For simplicity, let's assume that troves $n + 1, ..., n + m$ are the liquidated troves, in that order, and $1, ..., n$ are those that remain)

For a remaining trove:

$$x_i = x_i^{n+1} + \ldots + x_i^{n+m} = \sum_{k=n+1}^{n+m} x_i^k = \sum_{j=1}^{m} x_i^{n+j} \tag{13}$$

For a liquidated trove the sum would be truncated at the previous liquidated trove:

$$x_i = x_i^{n+1} + \ldots + x_i^{i-1} = \sum_{k=n+1}^{i-1} x_i^k \tag{14}$$

With each liquidation, c_j collateral is removed from the system. Again, as per (9), stake equals collateral. Thus, the S numerator in each liquidation is reduced by c_j, where j denotes the index of the liquidated trove.

Let

$$C_{n+m} = \sum_{i=1}^{n+m} c_i \tag{15}$$

and

$$L_m = \sum_{j=1}^{m} c_{n+j} \tag{16}$$

We now sum all reward events, noting that the liquidated trove's collateral is removed from the S denominator at each reward. Getting back to (13), note that for each previous liquidated trove $n+j$, the share of collateral that corresponds to trove i is:

$$x_i^j = \frac{c_i}{C_{n+m} - L_j}(c_{n+j} + x_{n+j}) \tag{17}$$

The denominator $C_{n+m} - L_j$ corresponds to the fact that the amount of total initial stakes has been reduced by the amount of liquidated collateral from troves until j, L_j. The collateral to redistribute is $c_{n+j} + x_{n+j}$, which corresponds to the initial collateral of the liquidated trove, c_{n+j}, plus the collateral it has earned from previous liquidations, x_{n+j}.

Therefore:

$$x_i = c_i \left[\frac{c_{n+1} + x_{n+1}}{C_{n+m} - L_1} + \frac{c_{n+2} + x_{n+2}}{C_{n+m} - L_2} + \frac{c_{n+3} + x_{n+3}}{C_{n+m} - L_3} + \ldots + \frac{c_{n+m} + x_{n+m}}{C_{n+m} - L_m} \right] \tag{18}$$

i.e.

$$x_i = c_i \sum_{j=1}^{m} \frac{c_{n+j} + x_{n+j}}{\sum_{i=1}^{n+m} c_i - \sum_{p=1}^{j} c_{n+p}} \tag{19}$$

(Note, that for liquidation of a given $trove_j$, the redistributed collateral is the sum of its collateral c_{n+j} plus it's accumulated collateral reward x_{n+j} which has itself been earned from liquidations $[n+1, n+2, n+3, \ldots n+j-1]$. Thus, liquidations have a "roll-up" effect - though, it is not important for our result. In fact, it can also be proved that $x_i = c_i \frac{L_m}{C_n}$)

We label the main sum expression H.

Rewriting $trove_i$'s accumulated reward:

$$x_i = Hc_i \tag{20}$$

Summing over all n active troves gives the total accumulated rewards for active troves in the system:

$$X_n = \sum_{i=1}^{n} Hc_i \tag{21}$$

$$X_n = H\,C_n \tag{22}$$

Note that after m liquidations, the system snapshots update from initially:

$$S_\emptyset = C_\emptyset = C_{n+m} \tag{23}$$

to:

$$S_\emptyset = C_n \tag{24}$$

$$C_\emptyset = C_n + X_n \tag{25}$$

(Note that it can also be proved that that $X_n = L_m$ and therefore $C_\emptyset = C_n + L_m = C_{n+m}$)

Now, a fresh trove is added, $trove_F$, with collateral c_F. Let the ICR of $trove_F$ equal the ICR of an active first-order $trove_G$.

Now, $trove_Z$ liquidates. Upon liquidation, the second-order $trove_F$ and the first-order $trove_G$ earn the following collateral rewards:

$$ICR_F = ICR_G \tag{26}$$

$$ICR_F = \frac{c_F}{d_F} \tag{27}$$

$$ICR_G = \frac{c_G + x_G}{d_G + y_G} \tag{28}$$

Where c_F, d_F and c_G, d_G are the collateral and debt values of $trove_F$ and $trove_G$ respectively.

x_G, y_G are the respective accumulated collateral and debt rewards for $trove_G$ earned by its stake over its lifetime.

The ICR equality identity (26) yields the following relation:

$$c_F = \frac{d_F}{d_G + y_G}(c_G + x_G) \tag{29}$$

i.e.

$$c_F = k(c_G + x_G) \tag{30}$$

where

$$k = \frac{d_F}{d_G + y_G} \tag{31}$$

$trove_F$'s stake s_F is given by the corrected stake rule (9), that is:

$$s_F = \frac{c_F \cdot S_\emptyset}{C_\emptyset} \tag{32}$$

Which by (24) and (25) gives:

$$s_F = \frac{c_F \cdot C_n}{C_n + X_n} \tag{33}$$

Now, a new liquidation occurs: $trove_Z$ liquidates. The system becomes second-order.

The event causes $trove_Z$'s collateral and debt (c_Z and d_Z) to be redistributed between all active troves, proportional to their stake.

For simplicity, let :

$$a = \frac{c_Z + x_Z}{S} \tag{34}$$

$$b = \frac{d_Z + y_Z}{S} \tag{35}$$

We define the collateral and debt rewards earned by $trove_F$ and $trove_G$ in the reward event:

$$\begin{aligned} r_{cF} &= a s_F \\ r_{dF} &= b s_F \\ r_{cG} &= a s_G \\ r_{dG} &= b s_G \end{aligned} \tag{36}$$

where

$$a = \frac{c_Z + x_Z}{S} \tag{37}$$

$$b = \frac{d_Z + y_Z}{S} \tag{38}$$

And since s_G is a first-order stake:

$$s_G = c_G \tag{39}$$

To show ICR equivalence after the reward event, we must first obtain s_F as a linear function of c_G. Recall our definition of $trove_F$'s stake from (33):

$$s_F = \frac{c_F \cdot C_n}{(C_n + X_n)} \tag{40}$$

Now, substituting in the expression for F's collateral, (30), we obtain:

$$s_F = \frac{k(c_G + x_G)C_n}{C_n + X_n} \tag{41}$$

Substituting in the expressions for accumulated reward x_i from (20), and total accumulated reward X_n from (22):

$$s_F = \frac{k(c_G + Hc_G)C_n}{C_n + HC_n} \tag{42}$$

And factorizing:

$$s_F = \frac{kc_G(C_n + HC_n)}{(C_n + HC_n)} \tag{43}$$

Canceling yields:

$$s_F = kc_G \tag{44}$$

We now compare ICRs of $trove_F$ and $trove_G$, after liquidation of $trove_Z$.

$$ICR_{F\ After} = \frac{c_F + r_{cF}}{d_F + r_{dF}} \tag{45}$$

$$ICR_{G\ After} = \frac{c_G + x_G + r_{cG}}{d_G + y_G + r_{dG}} \tag{46}$$

Using (36), the individual rewards as functions of stakes:

$$ICR_{F\ After} = \frac{c_F + as_F}{d_F + bs_F} \tag{47}$$

$$ICR_{G\ After} = \frac{c_G + x_G + as_G}{d_G + y_G + bs_G} \tag{48}$$

Now, substituting our definitions for s_G (39) and s_F (44):

$$ICR_{F\ After} = \frac{c_F + akc_G}{d_F + bkc_G} \tag{49}$$

$$ICR_{G\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{50}$$

Using identities (30) for c_F, and (31) for d_F:

$$ICR_{F\ After} = \frac{k(c_G + x_G + ac_G)}{k(d_G + y_G + bc_G)} \tag{51}$$

$$ICR_{G\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{52}$$

Cancelling k:

$$ICR_{F\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{53}$$

$$ICR_{G\ After} = \frac{c_G + x_G + ac_G}{d_G + y_G + bc_G} \tag{54}$$

Thus:

$$ICR_{F\ After} = ICR_{G\ After} \tag{55}$$

□

Lemma 6.2. *Arbitrary Number of Liquidation Events At Current System Order*

Proof. If instead of a single liquidation event at a given system order, we have P liquidation events, it is clear that ICR equality holds across all P events:

Since ICR equality holds across one liquidation event, it will hold across the next, and thus hold for all.

Liquidation events do not alter the stakes that earn shares of liquidated collateral and debt - and for a given stake, the individual trove reward term x_i given in 4) depends only on reward sizes and the total stakes. □

Lemma 6.3. *Arbitrary Number of troves Added Between Liquidation Events*

Proof. With N second-order troves added between consecutive liquidation events, the stake s_F of any given second-order trove is given by 1):

$$s_F = \frac{c_F \cdot S_\emptyset}{C_\emptyset} \tag{56}$$

The snapshots of the system state after the last liquidation event $(S_\emptyset, C_\emptyset)$ remain constant until the next liquidation. It is clear that all N second-order stakes s_F have been corrected by the same constant factor.

Thus, s_F in the N second-order troves case is equal to s_F in the single second-order trove case.

As such, the logic of the Main Proof applies - and ICR equality between a second-order trove and first-order trove holds across a liquidation event, no matter how many fresh troves are added in between. □

Theorem 6.4. *In a second order system with M previous liquidations, and N second-order troves added after the last liquidation, ICR equality between a first-order trove and second-order trove holds across P subsequent liquidation events*

Proof. Combining the previous 3 lemmas, this follows immediately. □

Lemma 6.5. *2nd Order Systems Collapse to 1st Order*

Proof. We now show that a second-order system is equivalent to a first-order system.

Consider a hypothetical first order $trove_1$ and an actual second order $trove_2$. Let both troves have identical ICR, and also let $trove_1$'s total collateral and debt equal $trove_2$'s initial collateral and initial debt respectively:

$$c_1 + x_1 = c_2 \tag{57}$$

$$d_1 + y_1 = d_2 \tag{58}$$

Clearly, the ratio $k = \frac{d_2}{(d_1 + y_1)} = 1$.

We substitute $k = 1$ into the second-order system expression for s_F, from equation 55), to yield:

$$s_2 = c_1 \tag{59}$$

11

Thus, any second-order stake is equivalent to some hypothetical first-order stake $s_1 = c_1$, which has accumulated collateral reward $x_1 = (c_2 - c_1)$ and debt reward $y_1 = (d_2 - d_1)$.

Therefore any second order system is equivalent to a first order system that contains only first-order stakes which have experienced all liquidations. We write:

$$\Gamma_2 = \Gamma_1 \tag{60}$$

$\square$

Proposition 6.6. *N'th Order Systems Collapse to 1st Order*

Proof. We prove it by induction. We have already proved for $n = 1$ that $\Gamma_1 = \Gamma_2$. Now we show that if it's true for $n - 1$ then it's true for n, i.e.:

$$\Gamma_{n-1} = \Gamma_n \Rightarrow \Gamma_n = \Gamma_{n+1} \tag{61}$$

Recall our system evolution function:

$$f(\Gamma_N) = \Gamma_{N+1} \tag{62}$$

Therefore:

$$\Gamma_{N+1} = f(\Gamma_N) = f(\Gamma_{n-1}) = \Gamma_N \tag{63}$$

So, for every N, $\Gamma_N = \Gamma_{N-1}$, and for the transitive property of equivalence, we finally have:

$$\Gamma_N = \Gamma_1 \tag{64}$$

$\square$

Having shown all nth order systems are equivalent to a first order system, we now extend our previous conclusion to nth order systems:

Corollary 6.6.1. *In an nth order system with M previous liquidations, and N second-order troves added after the last liquidation, ICR equality between an $(n-1)^{th}$ order trove and n^{th} order trove holds across P liquidation events.*

7   Corrected Stake Approach Preserves Order

Theorem 7.1. *For every system Γ_N containing troves i and j with $\gamma_i > \gamma_j$ that transitions to Γ_{N+1}, the corrected stake approach maintains $\gamma_i > \gamma_j$.*

Proof. Here we show that ICR ordering is preserved with corrected stakes across a liquidation event.

We make use of the first-order equivalence result, namely, that with corrected stakes:

$$\Gamma_N = \Gamma_1 \tag{65}$$

i.e:

Any N'th order system of troves is equivalent to a first-order system of troves. For a given fresh trove with stake s_i and collateral c_i, the stake s_i is equivalent to some hypothetical first-order stake c_j which has accumulated collateral reward $x_j = (c_i - c_j)$ and debt reward $y_j = (d_i - d_j)$.

Due to this equivalence between first and N'th-order systems, if ordering is preserved for first-order systems, it is preserved for N'th order systems.

Now consider a first-order system of troves, with stakes equal to their initial collateral.

Let $trove_1$ and $trove_2$ be troves with initial collateral c_1, c_2 accumulated collateral and debt rewards x_1, y_1 and x_2, y_2 respectively:

$$ICR_1 = \frac{c_1 + x_1}{d_1 + x_1} \tag{66}$$

$$ICR_2 = \frac{c_2 + x_2}{d_2 + y_2} \tag{67}$$

Let their ICRs be such that:

$$ICR_1 > ICR_2 \tag{68}$$

Since, a first-order trove's collateral and debt rewards are always in direct proportion to its initial collateral, we can write the accumulated rewards as:

$$x_1 = Ac_1 \tag{69}$$

$$x_2 = Ac_2 \tag{70}$$

and

$$y_1 = Bc_1 \tag{71}$$

$$y_2 = Bc_2 \tag{72}$$

Where A is the sum of all 'collateral rewards per unit staked', and B is the sum of all 'debt rewards per unit staked'. This yields ICRs:

$$ICR_1 = c_1 \frac{1 + A}{d_1 + Bc_1} \tag{73}$$

$$ICR_2 = c_2 \frac{1 + A}{d_2 + Bc_2} \tag{74}$$

And the initial ICR inequality becomes:

$$c_1 \frac{1 + A}{d_1 + Bc_1} > c_2 \frac{1 + A}{d_2 + Bc_2} \tag{75}$$

Cross multiplying and cancelling the common denominator yields:

$$c_1 \left(1 + A\right)\left(d_2 + Bc_2\right) > c_2 \left(1 + A\right)\left(d_1 + Bc_1\right) \tag{76}$$

Then expanding:

$$c_1 \left(d_2 + Bc_2\right) > c_2 \left(d_1 + Bc_1\right) \tag{77}$$

$$c_1 d_2 + Bc_1 c_2 > c_2 d_1 + Bc_1 c_2 \tag{78}$$

And cancelling terms:

$$c_1 d_2 > c_2 d_1 \tag{79}$$

Finally yielding the result:

$$\frac{d_2}{c_2} > \frac{d_1}{c_1} \tag{80}$$

We will later use this to prove that the inequality of ICRs holds across a liquidation event.

Now consider a liquidation event occurs. Upon a trove liquidation, r_c collateral and r_d debt are distributed to all active troves. Each active trove earns rewards proportional to its initial collateral, thus:

$$ICR_{1After} = \frac{c_1\left(1 + A\right) + ac_1}{d_1 + Bc_1 + bc_1} \tag{81}$$

$$ICR_{2After} = \frac{c_2\left(1 + A\right) + ac_2}{d_2 + Bc_2 + bc_2} \tag{82}$$

Where:

$$a = \frac{r_c}{S} \tag{83}$$

$$b = \frac{r_d}{S} \tag{84}$$

Collecting terms:

$$ICR_1 = \frac{c_1\left(1 + a + A\right)}{d_1 + \left(1 + B\right)c_1} \tag{85}$$

$$ICR_2 = \frac{c_2\left(1 + a + A\right)}{d_2 + \left(1 + B\right)c_2} \tag{86}$$

And taking reciprocals:

$$\frac{1}{ICR_{1After}} = \frac{d_1 + \left(1 + B\right)c_1}{c_1\left(1 + a + A\right)} \tag{87}$$

$$\frac{1}{ICR_{2After}} = \frac{d_2 + \left(1 + B\right)c_2}{c_2\left(1 + a + A\right)} \tag{88}$$

Rearranging, and separating the constant term:

$$\frac{1}{ICR_{1After}} = \left[\frac{\frac{d_1}{c_1}}{1 + a + A}\right] + \left[\frac{1 + B}{1 + a + A}\right] \tag{89}$$

$$\frac{1}{ICR_{2After}} = \left[\frac{\frac{d_2}{c_2}}{1 + a + A}\right] + \left[\frac{1 + B}{1 + a + A}\right] \tag{90}$$

Recall our earlier result (80): $\frac{d_1}{c_1} < \frac{d_2}{c_2}$. Thus:

$$\frac{1}{ICR_{1After}} < \frac{1}{ICR_{2After}} \tag{91}$$

Then taking reciprocals, finally yields:

$$ICR_{1After} > ICR_{2After} \tag{92}$$

Therefore, trove ordering holds across a liquidation event in first-order systems, and thus holds across a liquidation event in N'th order systems.

References

[1] R. Lauko, R. Pardoe. *Liquity: Decentralized Borrowing Protocol (Whitepaper), 2020.* https://docsend.com/view/bwiczmy

[2] B. Batog, L. Boca, N. Johnson. *Scalable Reward Distribution on the Ethereum Blockchain, 2018.* http://batog.info/papers/scalable-reward-distribution.pdf

8 Appendix

We prove that after a redistribution proportional to the collateral of active troves, the ordering of active troves by ICR is preserved.

Consider two active troves i and j with ICR γ_i, γ_j such that $\gamma_i > \gamma_j$.

Let c_i, d_i and c_j, d_j denote the collateral and debt of troves i and j respectively, and let C denote the total active collateral in the system.

Given the definition of ICR we have

$$\frac{c_i}{d_i} > \frac{c_j}{d_j} \tag{93}$$

In the event of a redistribution of a trove k, its collateral c_k and debt d_k is redistributed to all active troves, proportional to their shares of C.

Troves i and j thus receive the following pairs of collateral and debt rewards (x_i, y_i) and (x_j, y_j):

$$(x_i, y_i) = \left(\frac{c_i}{C} \cdot c_k, \frac{c_i}{C} \cdot d_k \right) \tag{94}$$

$$(x_j, y_j) = \left(\frac{c_j}{C} \cdot c_k, \frac{c_j}{C} \cdot d_k \right) \tag{95}$$

As a result, their ICRs will change to:

$$\gamma_i' = \frac{c_i + x_i}{d_i + y_i} \tag{96}$$

$$\gamma_j' = \frac{c_j + x_j}{d_j + y_j} \tag{97}$$

Let $a = \frac{c_k}{C}$ and $b = \frac{d_k}{C}$. Substituting the rewards, this leads to:

$$\gamma_i' = \frac{c_i + a \cdot c_i}{d_i + b \cdot c_i} \tag{98}$$

$$\gamma_j' = \frac{c_j + a \cdot c_j}{d_j + b \cdot c_j} \tag{99}$$

The equations 98 and 99 can be rewritten as:

$$\frac{1}{\gamma_i'} = \left(\frac{d_i}{c_i} + b \right) \cdot \frac{1}{1 + a} \tag{100}$$

$$\frac{1}{\gamma_j'} = \left(\frac{d_j}{c_j} + b \right) \cdot \frac{1}{1 + a} \tag{101}$$

Taking the reciprocal of inequality 93:

$$\frac{d_i}{c_i} < \frac{d_j}{c_j} \tag{102}$$

and applying it to equations 100 and 101, cancelling out common constants, yields:

$$\frac{1}{\gamma_i'} < \frac{1}{\gamma_j'} \tag{103}$$

Finally, taking the reciprocal of 103, yields:

$$\gamma_i' > \gamma_j' \tag{104}$$

Thus, ordering of active troves by ICR is preserved across a reward event that is proportional to the collateral of the active troves. $\qquad\square$