# NOTES ON PROOFGOLD REWARD BOUNTY CONJECTURES

CHAD E. BROWN

The Proofgold[1] consensus algorithm sends half of each block reward as a bounty to a Reward Bounty Conjecture [1]. One kind of bounty conjecture is related to The AIM Conjecture [2]. An analysis of the current conjectures in this class reveals that some are very easy and others are as hard as (half of) The AIM Conjecture itself. We give an obvious fix to prevent very easy conjectures. Using loops of small size (5, 6 and 7), we give estimates on how to modify the problems so that a probability of having a countermodel can be targeted. We also suggest a way of combining the loop problems with the existence of Ramsey graphs as a way of making the problems more likely to be difficult. We end with a hard fork proposal.

## 1. Loops and Inner Mappings

Loops are given by a carrier set $Q$, an identity element $e \in Q$, and three binary operations $\cdot$, $\backslash$ and $/$ on $Q$ satisfying certain laws. Given a loop certain families of inner mappings $T_x$, $L_{x,y}$ and $R_{x,y}$ can be defined. A loop is AIM if all inner mappings commute. It turns out that the inner mappings of the form $T_x$, $L_{x,y}$ and $R_{x,y}$ generate all inner mappings, so it is enough to say each of these commute (essentially giving six parameterized equations).

Proofgold also considers four other families of inner mappings:

- $I^1_x u = x \cdot (u \cdot (x \backslash e))$.
- $J^1_x u = ((e/x) \cdot u) \cdot x$.
- $I^2_x u = (x \backslash u) \cdot ((x \backslash e) \backslash e)$.
- $J^2_x u = (e/(e/x)) \cdot (u/x)$.

## 2. Candidate Counterexamples

The AIM related Proofgold bounty conjectures all state that every loop where some inner mappings commute and some inner mappings have a small finite order must satisfy one of the following two conclusions:

(1) $(L_{x,y} u \backslash e) \cdot u$ commutes with all elements.
(2) $(e/u) \cdot R_{x,y} u$ is in the middle nucleus.

The relationship to The AIM Conjecture is that if the two conclusions above hold for every AIM loop, then The AIM Conjecture follows. We say a loop is a *candidate counterexample of type 1* if there exist $x, y, u, w$ such that $((L_{x,y} u \backslash e) \cdot u) \cdot w$ and $w \cdot ((L_{x,y} u \backslash e) \cdot u)$ are different. We say a loop is a *candidate counterexample of type 2* if there

*Date*: October 16, 2020.
Czech Technical University in Prague.
[1] proofgold.org

exist $x, y, u, z, w$ such that $z \cdot (((e/u) \cdot R_{x,y}u) \cdot w)$ and $(z \cdot ((e/u) \cdot R_{x,y}u)) \cdot w$ are different. We say a loop is a *candidate counterexample* if it is a candidate counterexample of type 1 or of type 2.

There are no candidate counterexamples of cardinality less than 5. Of cardinality 5, there are 6 loops (up to isomorphism). All except the group $Z_5$ is a candidate counterexample. In fact all the nongroups of cardinality 5 are candidate counterexamples of both types. Of cardinality 6, there are 109 loops. Of these, 95 are candidate counterexamples of type 1 and 101 are candidate counterexamples of type 2, with a total of 104 candidate counterexamples. There are 23746 loops of cardinality 7, one of which is the group $Z_7$. Every loop of cardinality 7 except $Z_7$ is a candidate counterexample of type 1. Among these all but 16 are also candidate counterexamples of type 2.

In total there are 23854 candidate counterexamples of cardinality at most 7.

## 3. Inner Mapping Hypotheses

There are two kinds of hypotheses briefly mentioned above. The first is that "some" inner mappings commute. This is realized by randomly choosing some collections of inner mappings from the families above, composing them, and then asserting that pairs of the compositions commute. The second is that "some" inner mappings have a small finite order. This is realized by randomly choosing some collections of inner mappings, composing them between 2 and 5 times, and asserting that the result is the identity mapping. All AIM loops will satisfy the first kind of hypotheses, but not all AIM loops will satisfy the second kind.

Let us first note the flaw in the second kind of hypotheses. Suppose we randomly choose the inner mapping given by $T_x L_{y,z}$ and assert that $(T_x L_{y,z})^4$ is the identity mapping. Let us next suppose we randomly choose the inner mapping $R_{x,y}T_z$ and assert that $(R_{x,y}T_z)^3$ is the identity mapping. Note that $L_{e,e}$ and $R_{e,e}$ are the identity mapping and so we can infer $(T_x)^4$ and $(T_x)^3$ are the identity mapping. It follows that $T_x$ is the identity mapping since its order must divide both 3 and 4. If $T_x$ is the identity mapping for all $x$, then the loop is commutative. In this case the loop is trivially not a candidate counterexample of type 1.

Under similar pairs of assumptions about the orders of inner mappings it is often easy to infer $L_{x,y}$ or $R_{x,y}$ is the identity mapping implying the loop is associative. No associative loop is a candidate counterexample of type 2.

Due to these observations many of the AIM related reward bounty propositions are easily provable. One can ignore the hypotheses saying certain inner mappings commute and simply combine the hypotheses that some inner mappings have a small finite order to prove the loop must be commutative or associative. Combining this with the assumption that the loop is a candidate counterexample of type 1 or 2 gives a contradiction.

A simple way to prevent generating these trivial cases is to have at most *one* hypothesis stating some inner mappings have a small finite order.

Let us next note flaws in the first kind of hypotheses. Since $T_e$, $L_{x,e}$, $L_{e,x}$, $R_{x,e}$ and $R_{e,x}$ are always the identity mapping, assumptions above composed inner mappings commuting can be instantiated in ways that say many simpler inner mappings commute.

For example, suppose we, as above, randomly consider $T_x L_{y,z}$ and $R_{x,y} T_z$. In this case we say the two kinds of inner mappings commute:

$$T_{x_1} L_{y_1,z_1} R_{x_2,y_2} T_{z_2} = R_{x_2,y_2} T_{z_2} T_{x_1} L_{y_1,z_1}.$$

By specializing in different ways we can infer

$$T_{x_1} T_{z_2} = T_{z_2} T_{x_1},$$

$$L_{y_1,z_1} T_{z_2} = T_{z_2} L_{y_1,z_1},$$

$$T_{x_1} R_{x_2,y_2} = R_{x_2,y_2} T_{x_1}$$

and

$$L_{y_1,z_1} R_{x_2,y_2} = R_{x_2,y_2} L_{y_1,z_1}.$$

That is, from one hypothesis about randomly generated kinds of inner mappings commuting we have inferred four of the six conditions sufficient to require the loop to be an AIM loop. Due to this, it appears to be the case that many (probably most) of the randomly generated conditions do not say "some" inner mappings commute but that "all" inner mappings commute.

As a consequence it appears that AIM related reward bounty conjectures tend to fall into one of two classes: those which are trivial because the loop must be commutative or associative, and those which are only about AIM loops (making the problem almost as hard as the full AIM Conjecture).

One possible way to fix this second issue is to not generate compositions of independent inner mappings such as $R_{x,y} T_z$ but only compositions with dependencies such as $R_{x,y} T_{x \cdot y}$. Note that if $x$ or $y$ is $e$, then $R_{x,y}$ is simply the identity function so that $R_{x,y} T_{x \cdot y}$ is $T_y$ or $T_x$. If $x \cdot y$ is $e$, then $R_{x,y} T_{x \cdot y}$ is $R_{x, x\backslash e}$, a special case of $R$.

In addition, the current number of hypotheses about inner mappings commuting seems excessive. In total there are currently 20 identities of this form generated. In the next section we use evaluations on small candidate counterexamples to suggest that a smaller number of identities would be more appropriate.

## 4. Identities and Candidate Counterexamples

A *nominated inner mapping with one parameter* is either $T_x$, $I^1_x$, $J^1_x$, $I^2_x$ or $J^2_x$. A *nominated inner mapping with two parameters* is either $L_{x,y}$ or $R_{x,y}$. A *nominated operation* is one of the following sixteen binary operations (on $x$ and $y$):

| $x \cdot y$ | $x\backslash y$ | $x/y$ | $(y \cdot x)\backslash(x \cdot y)$ |
|---|---|---|---|
| $(x\backslash y)/x$ | $x\backslash(y/x)$ | $T_x y$ | $T_y x$ |
| $I^1_x y$ | $I^1_y x$ | $J^1_x y$ | $J^1_y x$ |
| $I^2_x y$ | $I^2_y x$ | $J^2_x y$ | $J^2_y x$ |

We consider the following families of identities:

- **$\mathbf{A}_0$:** $(F_{x,y} G_z H_w)^n u = u$ where $n \in \{2, 3, 4, 5\}$, $F$ is a nominated inner mapping with two parameters and $G$ and $H$ are nominated inner mappings with one parameter.

**A**$_1$**:** $(D_{x,y}G_zH_xF_{y,z})^nu = u$ where $n \in \{2,3,4,5\}$, $D$ and $F$ are nominated inner mappings with two parameters and $G$ and $H$ are nominated inner mappings with one parameter.

**A**$_2$**:** $(D_{x,y}G_zF_{x,y}H_z)^nu = u$ where $n \in \{2,3,4,5\}$, $D$ and $F$ are nominated inner mappings with two parameters and $G$ and $H$ are nominated inner mappings with one parameter.

**B:** $G_xH_y = H_yG_x$ where $G$ and $H$ are nominated inner mappings with one parameter.

**C:** $F_{x,y}G_z = G_zF_{x,y}$ where $F$ is a nominated inner mapping with two parameters and $G$ is a nominated inner mapping with one parameter.

**D:** $D_{x,y}F_{z,w} = F_{z,w}D_{x,y}$ where $D$ and $F$ are nominated inner mappings with two parameters. Note that these are always one of the conditions $LL$, $LR$ or $RR$.

**E**$_1$**:** $F_{x,f_1(y,z)}G^1_{f_2(x,z)}G^2_{g_1(w,v)}G^3_{g_2(w,v)} = G^2_{g_1(w,v)}G^3_{g_2(w,v)}F_{x,f_1(y,z)}G^1_{f_2(x,z)}$ where $F$ is a nominated inner mapping with two parameters, $G^1$, $G^2$ and $G^3$ are nominated inner mappings with one parameter and $f_1$, $f_2$, $g_1$ and $g_2$ are nominated operations.

**E**$_2$**:** $D_{x,f_1(x,y)}G_{f_2(x,f_3(y,z))}F_{w,v}H_{g(w,v)} = F_{w,v}H_{g(w,v)}D_{x,f_1(x,y)}G_{f_2(x,f_3(y,z))}$ where $D$ and $F$ are a nominated inner mappings with two parameters, $G$ and $H$ are nominated inner mappings with one parameter and $f_1$, $f_2$, $f_3$ and $g$ are nominated operations.

**F:** $D_{f_1(x,y),z}G^1_{f_2(x,z)}G^2_yF_{g_1(w,u),v}G^3_{g_2(u,v)} = F_{g_1(w,u),v}G^3_{g_2(u,v)}D_{f_1(x,y),z}G^1_{f_2(x,z)}G^2_y$ where $D$ and $F$ are a nominated inner mappings with two parameters, $G^1$, $G^2$ and $G^3$ are nominated inner mappings with one parameter and $f_1$, $f_2$, $g_1$ and $g_2$ are nominated operations.

For simplicity, we have combined the families $\mathbf{A}_0$, $\mathbf{A}_1$ and $\mathbf{A}_2$ into a single family **A** and combined the families $\mathbf{E}_1$ and $\mathbf{E}_2$ into a single family **E**. There are 1000 possible identities of type **A**, 25 possible identities of type **B**, 10 possible identites of type **C**, 3 possible identities of type **D**, almost 23 million possible identities of type **E** and over 32 million possible identities of type **F**. In order to estimate the probability of small candidate counterexamples satisfying the identities above, we consider all the identities of type **B**, **C** and **D** and a random selection of 100 identities of the other types. We evaluate these identities on all 5 candidate counterexamples of cardinality 5, all 104 candidate counterexamples of cardinality 6 and 68 randomly selected candidate counterexamples of cardinality 7. Table 1 shows the percentage of times a candidate counterexample satisfied an identity from the given family.

We can use these numbers to give very rough estimates for how often a finite loop satisfies a collection of identities from these classes. We estimate probabilities of combined events by simply multiplying probabilities, which is, of course, only valid assuming independence. One reason the estimates should only be considered "very rough" is that the events are definitely not independent. For example, $I^1_x$ can be expressed as $L_{x\backslash e,x}T_{x\backslash e}$. Consequently any loop satisfying $T_xT_y = T_yT_x$ from class **B** (for all $x, y$) and $T_xL_{y,z} = L_{y,z}T_x$ from class **C** (for all $x, y, z$) must satisfy $I^1_xT_y = T_yI^1_x$ from class **B**. Nevertheless, the hope is the estimates provide enough of a guide to choose the parameter settings below.

| | Size 5 | Size 6 | Size 7 | Total |
|---|---|---|---|---|
| **A** | 1% | 0.7% | 0 | 0.44% |
| **B** | 12.8% | 8.9% | 0.7% | 5.88% |
| **C** | 8% | 5.2% | 0 | 3.28% |
| **D** | 0 | 2.9% | 0 | 1.69% |
| **E** | 0.4% | 2.83% | 0.04% | 1.69% |
| **F** | 0 | 0.79% | 0 | 0.46% |

TABLE 1. How often a candidate counterexample satisfies an identity

| | $q_C^5$ | $q_C^6$ | $q_C^7$ | $q_C^{n<\omega}$ |
|---|---|---|---|---|
| **A** | 0.001 | 0.007 | 0 | 0.0044 |
| **B** | 0.128 | 0.089 | 0.007 | 0.0588 |
| **C** | 0.08 | 0.052 | 0 | 0.0328 |
| **D** | 0 | 0.029 | 0 | 0.0169 |
| **E** | 0.004 | 0.0283 | 0.0004 | 0.0169 |
| **F** | 0 | 0.0079 | 0 | 0.0046 |

TABLE 2. Estimated probabilities

Let us suppose we select an identity from each class $C$ with probability $p_C$, and do not select an identity with probability $1 - p_C$. Furthermore, let us say we try to select from class $C$ $n_C$ times, giving between 0 and $n_C$ identities from the class. Let $q_C$ be the probability that a candidate counterexample loop (possibly from a preselected population) satisfies an identity from $C$. The probability that a candidate counterexample loop satisfies the chosen set of identities can be computed as

$$p_C^{n_C} q_C^{n_C} + \binom{n-1}{n} p_C^{n_C-1}(1-p_C) q_C^{n_C-1} + \cdots + (1-p_C)^{n_C}.$$

For different choices of $n_C$ and $p_C$ for $C \in \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}, \mathbf{F}\}$ we can calculate estimates for the relevant probability using the values in Table 1 to estimate values of $q_C$. To be clear, Table 2 gives estimated values of $q_C$ when restricted to Size 5, Size 6, Size 7 or general sizes. We write $q_C^n$ for $q_C$ where the population is restricted to loops of cardinality $n$ and write $q_C^{n<\omega}$ where the population is all finite loops. The values for cardinalities 5 and 6 are most likely to be accurate since all candidate counterexamples were considered. The degree to which $q_C^{n<\omega}$ estimates are accurate when the data used only small loops is highly questionable, but our goal here is only to give rough estimates to justify possible choices of parameters.

In order to obtain probabilities of different orders of magnitude it will be enough to consider $p_C \in \{0.25, 0.5, 0.75, 1\}$ and $n_C \in \{1, 2, 3\}$. We only consider $n_{\mathbf{A}} = 1$ since $n_{\mathbf{A}} > 1$ risks forcing the loop to be commutative or associative as discussed in the previous section. Furthermore we only consider $p_{\mathbf{A}} = 0.75$ so that 25% of the choices will only include AIM identities and 75% will include an additional identity. To be more specific, 25% will contain an identity from $\mathbf{A}_0$, 25% will contain an identity from $\mathbf{A}_1$ and 25% will contain an identity from $\mathbf{A}_2$. In order to ensure a sufficient amount of

| $(n_{\mathbf{A}}, p_{\mathbf{A}}, n_{\mathbf{B}}, p_{\mathbf{B}}, n_{\mathbf{C}}, p_{\mathbf{C}}, n_{\mathbf{D}}, p_{\mathbf{D}}, n_{\mathbf{E}}, p_{\mathbf{E}}, n_{\mathbf{F}}, p_{\mathbf{F}})$ | estimated rarity |
|---|---|
| (1,0.75,3,0.25,2,0.25,2,0.25,4,1,3,0.5) | $10^9$ |
| (1,0.75,2,0.5,3,0.75,1,0.5,4,1,1,0.5) | $10^{10}$ |
| (1,0.75,3,0.25,1,0.25,1,1,4,1,2,0.75) | $10^{11}$ |
| (1,0.75,2,0.25,3,0.25,2,1,4,1,1,0.5) | $10^{12}$ |
| (1,0.75,1,0.5,1,0.25,3,0.25,4,1,2,1) | $10^{13}$ |
| (1,0.75,2,1,1,1,1,1,4,1,2,0.5) | $10^{14}$ |
| (1,0.75,3,0.25,3,0.75,3,1,4,1,2,0.5) | $10^{15}$ |
| (1,0.75,1,1,3,0.75,3,1,4,1,2,0.5) | $10^{16}$ |
| (1,0.75,3,1,1,1,2,1,4,1,1,0.75) | $10^{17}$ |
| (1,0.75,1,1,1,1,3,0.5,4,1,3,1) | $10^{18}$ |
| (1,0.75,3,1,2,0.75,3,1,4,1,2,0.75) | $10^{19}$ |
| (1,0.75,3,0.5,2,1,1,1,4,1,3,1) | $10^{20}$ |
| (1,0.75,1,1,3,1,3,1,4,1,1,1) | $10^{21}$ |
| (1,0.75,1,0.75,1,1,3,1,4,1,3,1) | $10^{22}$ |
| (1,0.75,2,1,1,0.75,3,1,4,1,3,1) | $10^{23}$ |

TABLE 3. Estimated rarity under parameter values

randomness in the selection of axioms, we will take $p_{\mathbf{E}}$ to be 1 and $n_{\mathbf{E}}$ to be 4, so that four identities are always chosen from $\mathbf{E}$. Table 3 gives values for $p_C$ and $n_C$ for each class along with the estimated number of candidate counterexample loops that would need to be considered before one satisfying a random collection of identities would be satisfied. These parameters could be used to implement the creation of random reward bounty propositions that are likely to be of increasing difficulty to resolve.

## 5. Ramsey Graphs

In order to make the reward bounty propositions more interesting, more varied and more likely to be difficult, we can combine the loop problems with the existence of Ramsey graphs. A Ramsey graph is a counterexample to $R(r, s) \leq n$, i.e., a graph with $n$ vertices where there is no clique of size $r$ and no anticlique of size $s$. An easy small example of a Ramsey graph is the graph $(V, E)$ with $V = \{a, b, c, d, e\}$ and

$$E = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e), (e, d), (e, a), (a, e)\}$$

ensuring $R(3, 3) > 5$. This Ramsey graph can be represented as a loop with a selected subset inducing the edges. Suppose $V$ is a loop with operation $\cdot$ and $X \subseteq V$. We say the *induced edge relation* is

$$E = \{(y, z) \in V \times V | \exists x \in X. x \cdot y = z \vee x \cdot z = y\}.$$

Another way to represent $E$ is using one of the division operations:

$$E = \{(y, z) \in V \times V | z/y \in X \vee y/z \in X\}.$$

Consider the loop with elements $\{a, b, c, d, e\}$ and operation

| $\cdot$ | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ |
| $b$ | $b$ | $d$ | $a$ | $e$ | $c$ |
| $c$ | $c$ | $e$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $c$ | $e$ | $b$ | $a$ |

Let $X$ be $\{a\}$. The induced edge relation contains the exactly the elements given in the Ramsey graph above:

$$E = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e), (e, d), (e, a), (a, e)\}.$$

These edges are supported by the second row of the table giving the operation. In general, $X$ will indicate a number of rows and will give an edge between each entry and the element indicating the column.

This method of inducing a graph from a loop and a selected subset is a generalization of Paley graphs. If $q$ is a prime with $q = 1 \mod 4$, then the Paley graph has vertices $\{0, \ldots, q-1\}$ where there is an edge between $y$ and $z$ if $y - z$ (modulo $q$) is a square in the finite field of order $q$. The graph about with 5 vertices is the Paley graph with $q = 5$. The Paley graph with $q = 17$ is the unique Ramsey graph ensuring $R(4, 4) > 17$. In our generalization we use a selected set $X$ in place of the set of squares and check if either $y/z$ or $z/y$ is in $X$ to ensure symmetry.

Let $U(r, s)$ be defined for $r, s \in \{3, 4, 5, 6\}$ where $r \leq s$ by the following table:

| $r\backslash s$ | 3 | 4 | 5 | 6 |
|---|---|---|---|---|
| 3 | 6 | 9 | 14 | 18 |
| 4 | | 18 | 25 | 41 |
| 5 | | | 48 | 87 |
| 6 | | | | 165 |

The value $U(r, s)$ is the largest possible value for $R(r, s)$ according to what is currently known about $R$. There are 381 conjectures of the form $R(r, s) > n$ where $r, s \in \{3, 4, 5, 6\}$, $n \in \{5, \ldots, 164\}$, $r \leq s$ and $n < U(r, s)$. Among these 102 are currently open mathematical conjectures.

To determine which are open we define $L(r, s)$ for $r, s \in \{3, 4, 5, 6\}$ where $r \leq s$ by the following table:

| $r\backslash s$ | 3 | 4 | 5 | 6 |
|---|---|---|---|---|
| 3 | 6 | 9 | 14 | 18 |
| 4 | | 18 | 25 | 36 |
| 5 | | | 43 | 58 |
| 6 | | | | 102 |

Here $L(r, s)$ is the smallest possible value for $R(r, s)$ according to what is currently known about $R$. If we could prove $R(r, s) > n$ where $n \geq L(r, s)$, then this would change what is currently known.

For some values of $(r, s, n)$ with low values of $n$ the conjectures are not interesting. To prove $R(5, 5) > 5$ only requires to give a graph with five vertices which has no 5-clique and no 5-anticlique. A graph with one edge suffices. To omit these obvious cases, let us further restrict to those with $n \geq r + s - 1$. This leaves 351 conjectures, with the 102 open conjectures still among these.

We can roughly order the triples $(r, s, n)$ by saying $(r_1, s_1, n_1) < (r_2, s_2, n_2)$ if

$$(o_1, r_1, s_1, n_1) < (o_2, r_2, s_2, n_2)$$

lexicographically, where $o_i$ is 1 if $R(r_i, s_i) > n_i$ is open and $o_i$ is 0 otherwise. This allows us to assign indices from 0 to 350 to the triples as shown in Tables 4, 5 and 6.

For each triple $(r, s, n)$ we can form a conjecture stating that no candidate counterexample of type 1 (or type 2) with $n$ elements satisfying some random identities as described previously has a subset $X$ that induces a Ramsey graph verifying $R(r, s) > n$. In order to prove such a conjecture, one would need to rule out all candidate counterexamples of cardinality $n$ satisfying the identities (which will be easy in case there are none). In order to prove the negation of such a conjecture, one needs to find a candidate counterexample with a selected subset $X$.

The difficulty of these conjectures can be partially parameterized by the values $(n_{\mathbf{A}}, p_{\mathbf{A}}, n_{\mathbf{B}}, p_{\mathbf{B}}, n_{\mathbf{C}}, p_{\mathbf{C}}, n_{\mathbf{D}}, p_{\mathbf{D}}, n_{\mathbf{E}}, p_{\mathbf{E}}, n_{\mathbf{F}}, p_{\mathbf{F}})$ determining how rare the appropriate candidate counterexample loops will be. As a second parameter we consider values $i \in \{0, \ldots, 223\}$. For a given value $i$ we choose at random a value $j \in \{i, \ldots, i + 127\}$ and use the triple with index $j$ from Tables 4, 5 and 6.

## 6. Four Classes of Problems at Different Levels of Difficulty

We now have four classes of problems each of which can be parameterized:

(1) AIM related conjectures of type 1 parameterized by $(n_{\mathbf{A}}, p_{\mathbf{A}}, n_{\mathbf{B}}, p_{\mathbf{B}}, n_{\mathbf{C}}, p_{\mathbf{C}}, n_{\mathbf{D}}, p_{\mathbf{D}}, n_{\mathbf{E}}, p_{\mathbf{E}}, n_{\mathbf{F}}, p_{\mathbf{F}})$.
(2) AIM related conjectures of type 2 parameterized by $(n_{\mathbf{A}}, p_{\mathbf{A}}, n_{\mathbf{B}}, p_{\mathbf{B}}, n_{\mathbf{C}}, p_{\mathbf{C}}, n_{\mathbf{D}}, p_{\mathbf{D}}, n_{\mathbf{E}}, p_{\mathbf{E}}, n_{\mathbf{F}}, p_{\mathbf{F}})$.
(3) Ramsey AIM related conjectures of type 1 parameterized by $(n_{\mathbf{A}}, p_{\mathbf{A}}, n_{\mathbf{B}}, p_{\mathbf{B}}, n_{\mathbf{C}}, p_{\mathbf{C}}, n_{\mathbf{D}}, p_{\mathbf{D}}, n_{\mathbf{E}}, p_{\mathbf{E}}, n_{\mathbf{F}}, p_{\mathbf{F}})$ and $i \in \{0, \ldots, 223\}$.
(4) Ramsey AIM related conjectures of type 2 parameterized by $(n_{\mathbf{A}}, p_{\mathbf{A}}, n_{\mathbf{B}}, p_{\mathbf{B}}, n_{\mathbf{C}}, p_{\mathbf{C}}, n_{\mathbf{D}}, p_{\mathbf{D}}, n_{\mathbf{E}}, p_{\mathbf{E}}, n_{\mathbf{F}}, p_{\mathbf{F}})$ and $i \in \{0, \ldots, 223\}$.

We propose a hard fork to update the generation of reward bounty conjectures to only generate those from the four classes above. Furthermore, we suggest increasing the difficulty in 15 phases using the parameters from Table 3. The $i$ parameter for the Ramsey problems can begin as 0 and be increased by 16 in each phase, with the final phase setting $i$ to 223 (instead of 224).

Each of the first fourteen phases could last 5000 blocks (roughly half a year). The fifteenth phase would be the final permanent phase.

## Acknowledgment

This work has been supported by the European Research Council (ERC) Consolidator grant nr. 649043 *AI4REASON*.

| | | |
|---|---|---|
| 0: (3,3,5) | 1: (3,4,6) | 2: (3,4,7) |
| 3: (3,4,8) | 4: (3,5,7) | 5: (3,5,8) |
| 6: (3,5,9) | 7: (3,5,10) | 8: (3,5,11) |
| 9: (3,5,12) | 10: (3,5,13) | 11: (3,6,8) |
| 12: (3,6,9) | 13: (3,6,10) | 14: (3,6,11) |
| 15: (3,6,12) | 16: (3,6,13) | 17: (3,6,14) |
| 18: (3,6,15) | 19: (3,6,16) | 20: (3,6,17) |
| 21: (4,4,7) | 22: (4,4,8) | 23: (4,4,9) |
| 24: (4,4,10) | 25: (4,4,11) | 26: (4,4,12) |
| 27: (4,4,13) | 28: (4,4,14) | 29: (4,4,15) |
| 30: (4,4,16) | 31: (4,4,17) | 32: (4,5,8) |
| 33: (4,5,9) | 34: (4,5,10) | 35: (4,5,11) |
| 36: (4,5,12) | 37: (4,5,13) | 38: (4,5,14) |
| 39: (4,5,15) | 40: (4,5,16) | 41: (4,5,17) |
| 42: (4,5,18) | 43: (4,5,19) | 44: (4,5,20) |
| 45: (4,5,21) | 46: (4,5,22) | 47: (4,5,23) |
| 48: (4,5,24) | 49: (4,6,9) | 50: (4,6,10) |
| 51: (4,6,11) | 52: (4,6,12) | 53: (4,6,13) |
| 54: (4,6,14) | 55: (4,6,15) | 56: (4,6,16) |
| 57: (4,6,17) | 58: (4,6,18) | 59: (4,6,19) |
| 60: (4,6,20) | 61: (4,6,21) | 62: (4,6,22) |
| 63: (4,6,23) | 64: (4,6,24) | 65: (4,6,25) |
| 66: (4,6,26) | 67: (4,6,27) | 68: (4,6,28) |
| 69: (4,6,29) | 70: (4,6,30) | 71: (4,6,31) |
| 72: (4,6,32) | 73: (4,6,33) | 74: (4,6,34) |
| 75: (4,6,35) | 76: (5,5,9) | 77: (5,5,10) |
| 78: (5,5,11) | 79: (5,5,12) | 80: (5,5,13) |
| 81: (5,5,14) | 82: (5,5,15) | 83: (5,5,16) |
| 84: (5,5,17) | 85: (5,5,18) | 86: (5,5,19) |
| 87: (5,5,20) | 88: (5,5,21) | 89: (5,5,22) |
| 90: (5,5,23) | 91: (5,5,24) | 92: (5,5,25) |
| 93: (5,5,26) | 94: (5,5,27) | 95: (5,5,28) |
| 96: (5,5,29) | 97: (5,5,30) | 98: (5,5,31) |
| 99: (5,5,32) | 100: (5,5,33) | 101: (5,5,34) |
| 102: (5,5,35) | 103: (5,5,36) | 104: (5,5,37) |
| 105: (5,5,38) | 106: (5,5,39) | 107: (5,5,40) |
| 108: (5,5,41) | 109: (5,5,42) | 110: (5,6,10) |
| 111: (5,6,11) | 112: (5,6,12) | 113: (5,6,13) |
| 114: (5,6,14) | 115: (5,6,15) | 116: (5,6,16) |

Table 4. Easiest Ramsey Triples

| | | |
|---|---|---|
| 117: (5,6,17) | 118: (5,6,18) | 119: (5,6,19) |
| 120: (5,6,20) | 121: (5,6,21) | 122: (5,6,22) |
| 123: (5,6,23) | 124: (5,6,24) | 125: (5,6,25) |
| 126: (5,6,26) | 127: (5,6,27) | 128: (5,6,28) |
| 129: (5,6,29) | 130: (5,6,30) | 131: (5,6,31) |
| 132: (5,6,32) | 133: (5,6,33) | 134: (5,6,34) |
| 135: (5,6,35) | 136: (5,6,36) | 137: (5,6,37) |
| 138: (5,6,38) | 139: (5,6,39) | 140: (5,6,40) |
| 141: (5,6,41) | 142: (5,6,42) | 143: (5,6,43) |
| 144: (5,6,44) | 145: (5,6,45) | 146: (5,6,46) |
| 147: (5,6,47) | 148: (5,6,48) | 149: (5,6,49) |
| 150: (5,6,50) | 151: (5,6,51) | 152: (5,6,52) |
| 153: (5,6,53) | 154: (5,6,54) | 155: (5,6,55) |
| 156: (5,6,56) | 157: (5,6,57) | 158: (6,6,11) |
| 159: (6,6,12) | 160: (6,6,13) | 161: (6,6,14) |
| 162: (6,6,15) | 163: (6,6,16) | 164: (6,6,17) |
| 165: (6,6,18) | 166: (6,6,19) | 167: (6,6,20) |
| 168: (6,6,21) | 169: (6,6,22) | 170: (6,6,23) |
| 171: (6,6,24) | 172: (6,6,25) | 173: (6,6,26) |
| 174: (6,6,27) | 175: (6,6,28) | 176: (6,6,29) |
| 177: (6,6,30) | 178: (6,6,31) | 179: (6,6,32) |
| 180: (6,6,33) | 181: (6,6,34) | 182: (6,6,35) |
| 183: (6,6,36) | 184: (6,6,37) | 185: (6,6,38) |
| 186: (6,6,39) | 187: (6,6,40) | 188: (6,6,41) |
| 189: (6,6,42) | 190: (6,6,43) | 191: (6,6,44) |
| 192: (6,6,45) | 193: (6,6,46) | 194: (6,6,47) |
| 195: (6,6,48) | 196: (6,6,49) | 197: (6,6,50) |
| 198: (6,6,51) | 199: (6,6,52) | 200: (6,6,53) |
| 201: (6,6,54) | 202: (6,6,55) | 203: (6,6,56) |
| 204: (6,6,57) | 205: (6,6,58) | 206: (6,6,59) |
| 207: (6,6,60) | 208: (6,6,61) | 209: (6,6,62) |
| 210: (6,6,63) | 211: (6,6,64) | 212: (6,6,65) |
| 213: (6,6,66) | 214: (6,6,67) | 215: (6,6,68) |
| 216: (6,6,69) | 217: (6,6,70) | 218: (6,6,71) |
| 219: (6,6,72) | 220: (6,6,73) | 221: (6,6,74) |
| 222: (6,6,75) | 223: (6,6,76) | 224: (6,6,77) |
| 225: (6,6,78) | 226: (6,6,79) | 227: (6,6,80) |
| 228: (6,6,81) | 229: (6,6,82) | 230: (6,6,83) |
| 231: (6,6,84) | 232: (6,6,85) | 233: (6,6,86) |
| 234: (6,6,87) | 235: (6,6,88) | 236: (6,6,89) |

Table 5. Intermediate Ramsey Triples

| | | |
|---|---|---|
| 237: (6,6,90) | 238: (6,6,91) | 239: (6,6,92) |
| 240: (6,6,93) | 241: (6,6,94) | 242: (6,6,95) |
| 243: (6,6,96) | 244: (6,6,97) | 245: (6,6,98) |
| 246: (6,6,99) | 247: (6,6,100) | 248: (6,6,101) |
| 249: (4,6,36) | 250: (4,6,37) | 251: (4,6,38) |
| 252: (4,6,39) | 253: (4,6,40) | 254: (5,5,43) |
| 255: (5,5,44) | 256: (5,5,45) | 257: (5,5,46) |
| 258: (5,5,47) | 259: (5,6,58) | 260: (5,6,59) |
| 261: (5,6,60) | 262: (5,6,61) | 263: (5,6,62) |
| 264: (5,6,63) | 265: (5,6,64) | 266: (5,6,65) |
| 267: (5,6,66) | 268: (5,6,67) | 269: (5,6,68) |
| 270: (5,6,69) | 271: (5,6,70) | 272: (5,6,71) |
| 273: (5,6,72) | 274: (5,6,73) | 275: (5,6,74) |
| 276: (5,6,75) | 277: (5,6,76) | 278: (5,6,77) |
| 279: (5,6,78) | 280: (5,6,79) | 281: (5,6,80) |
| 282: (5,6,81) | 283: (5,6,82) | 284: (5,6,83) |
| 285: (5,6,84) | 286: (5,6,85) | 287: (5,6,86) |
| 288: (6,6,102) | 289: (6,6,103) | 290: (6,6,104) |
| 291: (6,6,105) | 292: (6,6,106) | 293: (6,6,107) |
| 294: (6,6,108) | 295: (6,6,109) | 296: (6,6,110) |
| 297: (6,6,111) | 298: (6,6,112) | 299: (6,6,113) |
| 300: (6,6,114) | 301: (6,6,115) | 302: (6,6,116) |
| 303: (6,6,117) | 304: (6,6,118) | 305: (6,6,119) |
| 306: (6,6,120) | 307: (6,6,121) | 308: (6,6,122) |
| 309: (6,6,123) | 310: (6,6,124) | 311: (6,6,125) |
| 312: (6,6,126) | 313: (6,6,127) | 314: (6,6,128) |
| 315: (6,6,129) | 316: (6,6,130) | 317: (6,6,131) |
| 318: (6,6,132) | 319: (6,6,133) | 320: (6,6,134) |
| 321: (6,6,135) | 322: (6,6,136) | 323: (6,6,137) |
| 324: (6,6,138) | 325: (6,6,139) | 326: (6,6,140) |
| 327: (6,6,141) | 328: (6,6,142) | 329: (6,6,143) |
| 330: (6,6,144) | 331: (6,6,145) | 332: (6,6,146) |
| 333: (6,6,147) | 334: (6,6,148) | 335: (6,6,149) |
| 336: (6,6,150) | 337: (6,6,151) | 338: (6,6,152) |
| 339: (6,6,153) | 340: (6,6,154) | 341: (6,6,155) |
| 342: (6,6,156) | 343: (6,6,157) | 344: (6,6,158) |
| 345: (6,6,159) | 346: (6,6,160) | 347: (6,6,161) |
| 348: (6,6,162) | 349: (6,6,163) | 350: (6,6,164) |

Table 6. Hardest Ramsey Triples

## References

[1] Brown, C.E.: Hereditarily finite sets and Proofgold's consensus algorithm. Tech. rep., Czech Technical University in Prague (Aug 2020), http://grid01.ciirc.cvut.cz/~chad/pfghf.pdf

[2] Kinyon, M.K., Veroff, R., Vojtěchovský, P.: Loops with abelian inner mapping groups: An application of automated deduction. In: Bonacina, M.P., Stickel, M.E. (eds.) Automated Reasoning and Mathematics - Essays in Memory of William W. McCune. Lecture Notes in Computer Science, vol. 7788, pp. 151–164. Springer (2013)