Byzantine Fault Allowing: A Category of Fault-Tolerant State Machine Replica Protocols

Liam Monninger
liam@ramate.io
Ramate LLC
Durham, California, USA

Abstract

We define the category Byzantine Fault Allowing, denoted $\mathfrak{B}$, which formalizes fault-tolerant state machine replica protocols. We begin by motivating $\mathfrak{B}$ with developments in Byzantine fault-tolerant systems from both academia and industry. We then provide a theoretical motivation for $\mathfrak{B}$ by introducing approximations of a Byzantine majority algorithm B which later serves as a fixed-point in $\mathfrak{B}$. Building on this foundation, we define an initial form of $\mathfrak{B}$ and present several constructions within it. Finally, we discuss constructions of practical utility and benchmark those corresponding to implementable fault-tolerant systems.

CCS Concepts

• **Do Not Use This Code** → **Generate the Correct Terms for Your Paper**; *Generate the Correct Terms for Your Paper*; Generate the Correct Terms for Your Paper; Generate the Correct Terms for Your Paper.

Keywords

Byzantine Fault Allowing, Byzantine Fault Tolerance, State Machine Replication, Byzantine Fault Tolerant Systems

1 Introduction

1.1 Academia

1.2 Industry

2 Motivation

To motivate the category $\mathfrak{B}$, we perform a series of exercises. First, we consider a Byzantine majority algorithm, denoted

B, as a lossless expert model, representing a prospective fixed-point in $\mathfrak{B}$. Next, we consider combinatorial parameterizations of B, providing some initial morphisms on members of $\mathfrak{B}$. Finally, we examine a topological approximation of B, as an indication of non-trivial morphisms in $\mathfrak{B}$.

2.1 Expert Models, Byzantine Majorities, and B

To begin motivating structures of $\mathfrak{B}$, we argue that coordinating state machine replicas presents an online decision problem for which Byzantine majority presents a lossless expert model.

First, consider the information available in a state machine replica protocol. We know the following:

- There exists a set of replicas P which has disjoint subsets H and F such that $H \cap F = \emptyset$ and $H \cup F = P$.
- A client of the system will be able to obtain certificates of computed state transitions $r' \in R'$ from the replicas. We will denote these as $Q : R' \to 2^P$. Note that the value of $Val(Q(r')) = r'$ for all $r' \in R'$.
- To be a member of a quorum $Q(r')$, a replica must compute and broadcast the value r'.
- Honest nodes compute a correct state transition. Tautologically, a state transition is correct if the quorum of which it is a member intersects with the honest set $Q(r') \cap H \neq \emptyset$.

Now consider our objectives. We want:

- Our state transition is correct.
- Our state transition is consistent, i.e., records the past effects of previous state transitions.

Our determination for correctness Cor is given to us by our tautology above:

$$Cor(r') \triangleq (Q(r') \cap H \neq \emptyset)$$

Consistency is less obvious. For the purpose of this motivation, we will assume a sequence of state transitions $r'_1, r'_2, \cdots, r'_n$ which we will denote as R'. We will say that a quorum $Q(r'_j)$ is consistent if and only if its predecessor $Q(r'_{j-1})$ is consistent and the two quora intersect, i.e., $Q(r'_j) \cap Q(r'_{j-1}) \neq \emptyset$. Observe that the expansion of our consistency function Con records all the effects of previous state transitions satisfying our original semantic intent:

$$C(r_i', r_j') \triangleq (Q(r_i') \cap Q(r_j') \neq \emptyset)$$
$$Con(r_j') = Con(r_{j-1}') \wedge C(r_{j-1}', r_j')$$
$$= C(r_0', r_1') \wedge \cdots \wedge C(r_{j-1}', r_j')$$

We combine these definitions of correctness and consistency to form our objective Obj. Observe that the expansion records all correct effects of previous state transitions satisfying the original semantic intent:

$$O(r_i', r_j') \triangleq (Q(r_i') \cap Q(r_j') \cap H \neq \emptyset)$$
$$Obj(r_j') = Obj(r_{j-1}') \wedge O(r_{j-1}', r_j')$$
$$= Obj(r_0') \wedge O(r_0', r_1') \wedge \cdots \wedge O(r_{j-1}', r_j')$$
$$= Obj(r_0')$$
$$\wedge \, (Q(r_0') \cap Q(r_1') \cap H \neq \emptyset)$$
$$\cdots$$
$$\wedge \, (Q(r_{j-1}') \cap Q(r_j') \cap H \neq \emptyset)$$

We transform this into a loss function $Loss$ which counts the number of incorrect or inconsistent quora for our expert model as below. Note that later we will discuss alternative definitions of loss:

$$Loss(r_j') =$$
$$\sum_{r_i' \in [r_0', r_j']} [\neg Obj(r_i')]$$
$$= [\neg Obj(r_0')] + [\neg Obj(r_1')] + \cdots + [\neg Obj(r_j')]$$
$$= [\neg Obj(r_0')]$$
$$+ [Q(r_1') \cap Q(r_0') \cap H = \emptyset]$$
$$\cdots$$
$$+ [Q(r_j') \cap Q(r_{j-1}') \cap H = \emptyset]$$

Observe that the loss function $Loss$ is 0 if and only if the quorum $Q(r')$ is consistent and correct, i.e., $Obj(Q(r'), R') = 0$.

We now consider B which certifies any quorum surpassing $2f + 1$ replicas, under the assumption that at most f replicas are Byzantine. As we will show, this is a lossless expert model.

First, we restate the proof that any two quora must intersect in at least one honest replica:

THEOREM 2.1. *Given honest nodes compute and broadcast a correct state transition and that the set of replicas P contains:*

- *at least $2f + 1$ honest replicas,*
- *at most f Byzantine replicas.*

Any two quora $Q(r_1'), Q(r_2')$ will intersect in at least one honest replica.

PROOF. Let...
- P be the set of replicas,
- H be the subset of honest replicas,
- F be the subset of Byzantine replicas.

$$P = H \cup F$$
$$H \cap F = \emptyset$$

Let $Q : R' \to 2^P$ be the function which maps a state transition to the quorum obtained by the replicas which compute and broadcast a correct state transition.

Apply the Byzantine constraints that...
- $|Q(r')| \geq 2f + 1 \forall r' \in R'$.
- $|H| \geq 2f + 1$.
- $|F| \leq f$.
- $|H| + |F| = |P| = 3f + 1$.

For any two state transitions $r_1', r_2' \in R'$ by definition of the Byzantine constraints $|Q(r_1')| \geq 2f + 1$ and $|Q(r_2')| \geq 2f + 1$. It also follows that $3f + 1 \geq |Q(r_1') \cup Q(r_2')|$ as there cannot be more than $3f + 1$ replicas in total, of which the honest replicas H are a subset.

Two quora must then intersect in at least $f + 1$ replicas:

$$|Q(r_1') \cap Q(r_2')| =$$
$$|Q(r_1')| + |Q(r_2')|$$
$$- |Q(r_1') \cup Q(r_2')|$$
$$\geq (2f + 1) + (2f + 1)$$
$$- (3f + 1)$$
$$= f + 1$$

Likewise, the intersection of two quora must intersect in at least one honest replica:

$$|Q(r_1') \cap Q(r_2')|$$
$$= |Q(r_1') \cap Q(r_2') \cap H|$$
$$+ |Q(r_1') \cap Q(r_2') \cap F|$$
$$|Q(r_1') \cap Q(r_2') \cap H|$$
$$= |Q(r_1') \cap Q(r_2')|$$
$$- |Q(r_1') \cap Q(r_2') \cap F|$$
$$f \geq |Q(r_1') \cap Q(r_2') \cap F|$$
$$|Q(r_1') \cap Q(r_2') \cap H| \geq f + 1 - f = 1$$

$\square$

We now show inductively that the Byzantine majority is lossless.

THEOREM 2.2. *The Byzantine majority is lossless under the assumption that $Obj(Q(r_0'), R') = 1$.*

PROOF. **Base cases:**

- By assumption, $Q(r_0')$ is correct and consistent. Vacuously, any quorum surpassing $2f + 1$ replicas must contain at least $f+1$ honest replicas and is thus correct which holds for $Q(r_0')$. And, it does not have any predecessors. Thus, $Obj(Q(r_0'), R') = 1 \implies Loss(Q(r_0'), R') = 0$.

- $Obj(Q(r_1'), R') = Q(r_1') \cap Q(r_0') \cap H \neq \emptyset \implies Loss(Q(r_1'), R')$. By Thereom 1, any two quora must intersect in at least one honest replica. Thus, $Q(r_1') \cap Q(r_0') \cap H \neq \emptyset$. Thus, $Obj(Q(r_1'), R') = 1 \implies Loss(Q(r_1'), R') = 0$. All other inductive steps no longer need to directly consider the assumption that $Obj(Q(r_0'), R') = 1$.

Inductive step: Assume $Obj(Q(r_{j-1}'), R') = 1$. From our definition of Obj, we have that:

$$
\begin{aligned}
&Obj(Q(r_j'), R') \\
&\quad = Obj(Q(r_{j-1}'), R') \\
&\quad\quad \wedge Q(r_j') \cap Q(r_{j-1}') \cap H \neq \emptyset \\
&Obj(Q(r_{j-1}'), R') = 1 \implies \\
&Obj(Q(r_j'), R') \\
&\quad = 1 \wedge Q(r_j') \cap Q(r_{j-1}') \cap H \neq \emptyset
\end{aligned}
$$

Substituting from Thereom 1 we have $(Q(r_j') \cap Q(r_{j-1}') \cap H \neq \emptyset) = 1$. Thus, $Obj(Q(r_j'), R') = 1 \implies Loss(Q(r_j'), R') = 0$.

$\square$

B is a lossless expert model. In Appendix B, we further motivate the necessity of the Byzantine assumptions for any such lossless model to exist. However, given these assumptions, we may now consider how to approximate B.

2.2 Sampling Approximations of B

One simple approach to approximating B which may spring to the mind of the statistician is to sample those replicas which participate in the quora of B. That is, to pick at random from P a subset of replicas needed for a quorum and consider this in place of the supermajority of replicas required by B. As we will show, though this is trivial, it has appealing combinatorial properties.

For the sake of explanation, let our initial sampling algorithm be defined as follows:

- For a given index, n on R, pick a random subcommittee $K_n \subseteq P$ s.t. $|K_n| = 3k + 1$.
- Accept r' if and only if $|Q_{K_n}(r')| \geq 2k+1$ and $N(r') = n$. Note that we use Q' because we do not assume this subcommittee agrees.

Observe the following possible outcomes for selection of this subcommittee:

- $|K_n \cap H| \geq 2k + 1$. This represents a subcommittee which has an honest supermajority which computes r'

correctly. For ease of reference, we shall refer to this as kind of subcommittee as $Right$ and use the symbol $\mathcal{R}$.

- $k < |K_n \cap H| < 2k+1$. This represents a subcommittee that has neither an honest nor dishonest supermajority and may either compute r' correctly or disagree internally and not render a supermajority. For ease of reference, we shall refer to this as kind of subcommittee as $Hung$ and use the symbol $\mathcal{H}$.

- $|K_n \cap H| \leq k$. This represents a subcommittee which has a dishonest supermajority and may compute r' incorrectly. For ease of reference, we shall refer to this as kind of subcommittee as $Corrupt$ and use the symbol $\mathcal{C}$.

We shall now compute the probabilities of these outcomes. Let $\mathcal{S}(f, k)$ represent the total number of ways to select the subcommittee without replacement:

$$
\mathcal{S}(f, k) = \binom{3f + 1}{3k + 1}
$$

The total number of ways to select a $Corrupt$ subcommittee is:

$$
\mathcal{S}_{\mathcal{C}}(f, k) = \sum_{h=2k+1}^{\min(3k+1, f)} \binom{f}{h} \cdot \binom{2f + 1}{3k + 1 - h}
$$

The total number of ways to select a $Right$ subcommittee is:

$$
\mathcal{S}_{\mathcal{R}}(f, k) = \sum_{h=2k+1}^{\min(3k+1, 2f+1)} \binom{f}{h} \cdot \binom{f}{3k + 1 - h}
$$

All other outcomes are $Hung$, so the total number of ways to select a $Hung$ subcommittee is:

$$
\mathcal{S}_{\mathcal{H}}(f, k) = \mathcal{S}(f, k) - \mathcal{S}_{\mathcal{C}}(f, k) - \mathcal{S}_{\mathcal{R}}(f, k)
$$

Before we further refine our sampling algorithm, observe that the probability of selecting a $Right$ subcommittee is:

$$
Pr[\mathcal{R}](f, k) = \frac{\mathcal{S}_{\mathcal{R}}(f, k)}{\mathcal{S}(f, k)}
$$

All $Right$ subcommittees intersect with H and thus satisfy $Cor(r')\forall r' \in R'$. The probability of computing a correct state transition r' is then...

$$
Pr[Cor(r')](f, k) \geq Pr[\mathcal{R}](f, k)
$$

Unfortunately, the probability of selecting a *Right* subcommittee $Pr[\mathcal{R}](f,k)$ tends downwards towards $\frac{1}{2}$ as f increases for a fixed ratio $\gamma = \frac{k}{f}$.

> **[Liam Monninger]:** TODO: All of these limits need to re-formalized. For now, I'm just recording the results.

$$\lim_{f\to\infty} Pr[\mathcal{R}'](\gamma,k) = \frac{1}{2} \forall k \in \mathbb{N} : k < f$$

However, the probability of selecting a *Corrupt* subcommittee $Pr[\mathcal{C}'](\gamma,k)$ tends towards 0 as f increases for a fixed ratio $\gamma = \frac{k}{f}$.

$$\lim_{f\to\infty} Pr[\mathcal{C}'](\gamma,k) = 0 \forall k \in \mathbb{N} : k < f$$

This implies that the probability of selecting a *Hung* subcommittee $Pr[\mathcal{H}'](\gamma,k)$ tends towards $\frac{1}{2}$ as f increases for a fixed ratio $\gamma = \frac{k}{f}$.

$$\lim_{f\to\infty} Pr[\mathcal{H}'](\gamma,k) = \frac{1}{2} \forall k \in \mathbb{N} : k < f$$

We can use this information to consider the complexity of the sampling algorithm for a sampling ratio $\gamma = \frac{k}{f}$ denoted $\Theta(Sampling_\gamma)$ and later to refine our algorithm.

Observe the probability of rendering a decision $Pr[Accepted](f,k)$ which shall certainly occur if the subcommittee is either *Right* or *Corrupt* and may occur if the subcommittee is *Hung*.

$$Pr[Accepted](f,k) \geq Pr[\mathcal{R}](f,k) + Pr[\mathcal{C}](f,k)$$

Since $Pr[\mathcal{R}](f,k) > \frac{1}{2}$ and $Pr[\mathcal{C}](f,k) > 0$ for all $f, k \in k < f$, we have that $Pr[Accepted](f,k) > \frac{1}{2}$.

To ensure we render a decision, we devise a simple algorithm. We first attempt to sample. If K_n does not map to Q_{K_n}, we then ask the entire set of replicas P to compute r' and take the result of the supermajority. Under our Byzantine assumptions, the second step will always render a decision. Further, the second step has the complexity of the original Byzantine majority algorithm $\Theta(B_f) = 3f + 1$ as both use all replicas.

The expected complexity of the updated sampling algorithm $\Theta(\mathcal{B}_{f,k})$ is bounded by the complexity of B $\Theta(B_f)$. More specifically, we have that:

$$\Theta(\mathcal{B}_{f,k}) =$$
$$Pr[Accepted](f,k) \cdot (3k+1)$$
$$+ (1 - Pr[Accepted](f,k)) \cdot ((3f+1) + (3k+1))$$
$$= \frac{3k+1}{2} + \frac{(3f+1) + (3k+1)}{2}$$
$$= \frac{3f+1}{2} + 3k + 1$$
$$= \frac{\Theta(B_f)}{2} + 3k + 1$$

Via this naive sampling approach, we have already roughly halved the expected complexity of B. But, we can generalize and improve this approach by resampling. If for each *Hung* subcommittee we sample again, we can observe that the likelihood of needing to resample at any given step is $\frac{1}{2}$. Thus, the expected complexity of the sampling algorithm is:

$$Pr[\text{Resample Count} = n] = \left(1 - \frac{1}{2}\right)^{n-1} \cdot \frac{1}{2} = \frac{1}{2^n}$$
$$\Theta(\text{BFA}) = (3k+1) \cdot \mathbb{E}[\text{Resample Count}]$$
$$= (3k+1) \cdot \sum_{n=1}^{\infty} n \cdot \frac{1}{2^n}$$
$$= 2(3k+1) = 2\gamma \cdot \Theta(B_f)$$

In other words, on average, we would expect to use two subcommittees of size $3k + 1 = 3\gamma \cdot f + 1$ to render a decision.

Since each resampling is independent and our $Q'(r')$ after resampling cannot be *Hung*, the probability that the state transition r' is computed correctly is simply:

$$Pr[\mathcal{R}'](f,k) \triangleq 1 - Pr[\mathcal{H}'](f,k) - Pr[\mathcal{C}'](f,k)$$
$$Pr[\mathcal{H}'](f,k) = 0 \text{ by definition}$$
$$Pr[\mathcal{C}'](f,k) = Pr[\mathcal{C}](f,k) \text{ by independence}$$
$$Pr[Cor(r')](f,k) \geq Pr[\mathcal{R}'](f,k)$$
$$= 1 - Pr[\mathcal{C}](f,k)$$

Substituting and rearranging, we can describe the loss on the *Cor*, denoted *Closs*, due to sampling:

$$Closs(r'_j) \triangleq \sum_{r'_i \in [r'_0, r'_j]} [\neg Cor(r'_i)]$$
$$E_{\mathcal{B}_{f,k}}[Closs(r'_j)] = \sum_{r'_i \in [r'_0, r'_j]} Pr[\mathcal{C}](f,k)$$
$$= (j+1) \cdot Pr[\mathcal{C}](f,k)$$
$$= (j+1) \cdot \frac{\sum_{h=2k+1}^{\min(3k+1,f)} \binom{f}{h}\binom{2f+1}{3k+1-h}}{\binom{3f+1}{3k+1}}$$

For concision, we define $\alpha_{f,k} \triangleq Pr[\mathcal{C}](f,k)$ and state that $\mathcal{B}_{j,k}$ is $(j\alpha_{f,k})$-approximate w.r.t. $Closs$. As shown above, $j\alpha_{f,k}$ decreases exponentially for a fixed $\gamma = \frac{k}{f}$ as f increases. In practice, this implies that values of $Closs_{\mathcal{B}_{f,k}}(r'_j)$ that are comparable to cryptographic security standards can be achieved using only a fraction of the replicas, as shown in Figure 1. Replicas that are not involved may pre-compute elements of other state transitions, lending to horizontal scalability in the context of a distributed system.
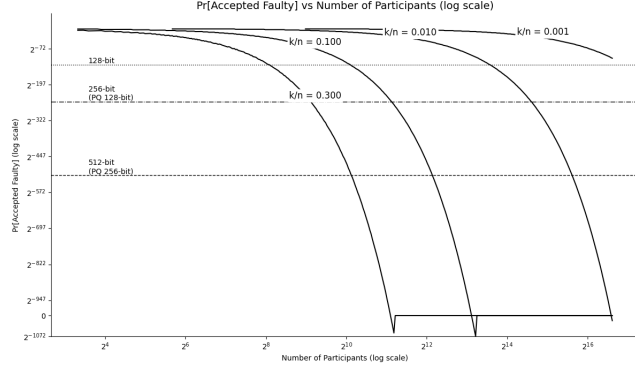
(a) The probability of selecting a $Corrupt$ subcommittee (Accepted Faulty) as a function of f and k (n in this out of date figure).
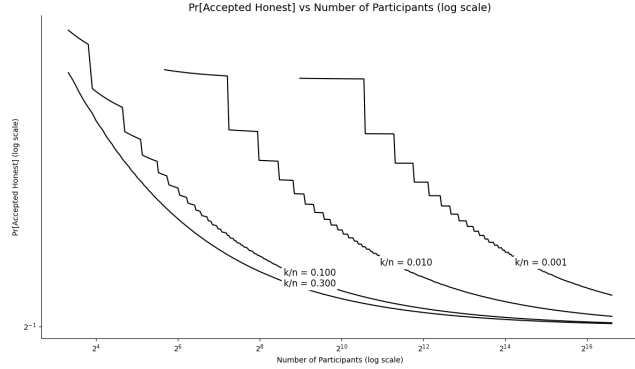
(b) The probability of selecting a $Right$ subcommittee (Accepted Honest) as a function of f and k (n in this out of date figure).

Figure 1: Probabilities of selecting $Corrupt$ and $Right$ subcommittees as functions of f and k.

Consistency, as defined by Con as the intersection of consecutive state transitions in an honest replica, is not as strongly approximated by $\mathcal{B}_{f,k}$. Consequently, $\mathcal{B}_{f,k}$ exhibits higher overall loss with respect to $Hloss$ and Obj, which we demonstrate more thoroughly in Appendix A.

As we shall continue to motivate via the topological considerations in the proceeding section and later unify in this paper's main theorem, we argue that these initial properties of $\mathcal{B}_{f,k}$ should be taken as indication of structure. There exist combinatorial parameterizations of B that can be composed,

as we have done in our resampling construction. Ultimately, these compositions may yield algorithms with subtle but potentially advantageous properties.

2.3 Topological Approximations of B

[Liam Monninger]: This section currently just riffing on some genres of projections and embeddings. It's nothing cohesive.

In the previous section, we described combinatorial parameterizations of B which may be considered trivial. To motivate a deeper sense of the category $\mathfrak{B}$, we now consider topological approximations of B. This approach concerns studying the shape of quorum to understand which points, polygons, and holes might be added or removed, and what effect this has on the $Loss$ of the approximate algorithm from B.

For the sake of exposition, we shall consider first several embeddings of the data of B into a space which may behave as a suitable metric space. All embeddings of B will be denoted by ϕ and begin with the following assumptions:

- By our initial definition of consistency Con, quora are indexed by the natural numbers $o : \mathbb{N} \leq |Q| \twoheadrightarrow Q$.
- We assume a bijection between the natural numbers and the replicas $p : \mathbb{N} \leq |P| \twoheadrightarrow P$.
- We assume a bijection between the natural numbers and the values $r' \in R$ denoted $r : \mathbb{N} \twoheadrightarrow R$.

Thus, we may naively project this into $\mathbb{R}^3$ by the identity inclusion $i(n) = n$ for each datum:

$$\phi_{r,o,p} : Q \to \mathbb{R}^3 = (i(r), i(o), i(p))$$

This projection captures the raw values of the quora. Notably, data reflecting the same value at the same quorum index by different replicas can be arbitrarily far apart. To rectify this, we can scale the projection by $|P|$:

$$\phi_{r,o,p} : Q \to \mathbb{R}^3 = (i(r), i(o), \frac{i(p)}{|P|})$$

This projection captures the values of the quora. Notably, however, points reflecting different quorum indexes and values from the same replica can be arbitrarily far apart. To rectify this, we can project pairwise commutations of the terms in $\phi_{r,o,p}$. We use $\cdot$ to mark an arbitrary commutator:

$$\phi_{r,o,p,\cdot} : Q \to \mathbb{R}^3 = (i(r) \cdot i(o), i(r) \cdot \frac{i(p)}{|P|}, i(o) \cdot \frac{i(p)}{|P|})$$

This correlates all components of the projection with each other. Alternatively, we can perform a non-commutative pairwise projection, denoted by $-$:

$$\phi_{r,o,p,-} : Q \to \mathbb{R}^6 = ($$
$$i(r) - i(o),$$
$$i(r) - \frac{i(p)}{|P|},$$
$$i(o) - i(r),$$
$$i(o) - \frac{i(p)}{|P|},$$
$$\frac{i(p)}{|P|} - i(r),$$
$$\frac{i(p)}{|P|} - i(o)$$
$$)$$

This correlates all components of the projection with each other while preserving information about the nature of the formation of the pairwise interaction.

Finally, we consider a Order-2 projection in which each $\phi_{r,o,p,T} : Q \to \mathbb{R}^{|P| \times 2}$ wherein each quorum index and value pair is inserted into the matrix at the index of the replica:

$$\phi_{r,o,T}(q) * j, 1 = \mathbf{1} * \rho_j \in q, i(o_{\rho_j}),$$
$$\phi_{r,o,T}(q) * j, 2 = \mathbf{1} * \rho_j \in q, \frac{i_T(p_{\rho_j})}{|P|}$$

> [**Liam Monninger**]: The richest space in which we may embed the data of B is $\mathbb{R}^{|P| \times 2}$. This space allows us to capture the most information about the data. However, it is also the most complex space and thus the most difficult to work with.
> Playing with writing the algorithm over the other spaces is a fun exercise. Beginning with trivial projections and implementations, and morphing to more complex ones, then approximating is a reflection of the category we're trying to build.

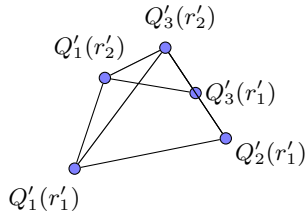For each of these projections, we can anaylze the data of B as a simplicial complex shown in Figure 2.

Figure 2: A simplicial complex representing the data of B for three replicas on state transitions r_1' and r_2'.

3 Byzantine Fault Allowing

We define the category Byzantine Fault Allowing, denoted $\mathfrak{B}$, as the category of fault-tolerant parametric state machine replica protocols. In the proceeding subsections, we first re-examine our approximations of B as categorical constructions. We then generalize to provide the definition of $\mathfrak{B}$. Finally, we identify additional elementary constructions which will be leveraged in the section on constructions and implementations.

3.1 Combinatorial Morphisms and the Fixed Point B

For the sake of exposition, let $\mathcal{D} \hookrightarrow \mathfrak{B}$ represent a subcategory of $\mathfrak{B}$ s.t. $\mathrm{Ob}(\mathcal{D})$ represent resampling parameterizations of B described in the previous section. We will formalize $\mathcal{D}$ later.

Assume also any algorithm A which produces quora $Q_B(r') \subseteq Q_A(r')$ is equivalent to B.

We can describe a morphism $\lceil : \mathrm{Ob}(\mathcal{D}) \to \mathrm{Ob}(\mathcal{D})$ which takes a resampling algorithm $X_{k,f}$ using the resampling parameters k and f and increments k by 1. That is...

$$\lceil : \mathrm{Ob}(\mathcal{D}) \to \mathrm{Ob}(\mathcal{D})$$
$$\lceil(X_{k,f}) = X_{k+1,f}$$

This implies that after $f - k$ such morphisms, we will have produced the algorithm $X_{f,f}$ which is equivalent to B. Further application of $\lceil$ will yield the algorithm $X_{f+1,f}$ which is also equivalent to B. This implies that $B = X_{f,f}$ is a fixed point of $\mathcal{D}$ in the category $\mathfrak{B}$.

$$X_{k,f} \in \mathcal{D} \xrightarrow{\lceil} \cdots f - k \cdots \xrightarrow{\lceil} B \circlearrowleft \lceil$$
$$X_{f-1,f} \in \mathcal{D}$$

4 Constructions and Implementations

5 Conclusion

Acknowledgments