BFA: Byzantine Fault Allowing Parametric State Machine Replicas

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

Abstract

We define a category Byzantine Fault Allowing, denoted $\mathfrak{B}$, which formalizes fault-tolerant parametric 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

Do, Not, Use, This, Code, Put, the, Correct, Terms, for, Your, Paper

ACM Reference Format:
Liam Monninger. 2025. BFA: Byzantine Fault Allowing Parametric State Machine Replicas. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX)*. ACM, New York, NY, USA, 9 pages. https://doi.org/XXXXXXX.XXXXXXX

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

2.1 Expert Models and the Byzantine Generals Problem

To begin in motivating the 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:

Conference acronym 'XX, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/XXXXXXX.XXXXXXX

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

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:

$$
\begin{aligned}
&O(r_i', r_j') \triangleq (Q(r_i') \cap Q(r_j') \cap H \neq \emptyset) \\
&Obj(r_j') = Obj(r_{j-1}') \wedge O(r_{j-1}', r_j') \\
&\quad = Obj(r_0') \wedge O(r_0', r_1') \wedge \cdots \wedge O(r_{j-1}', r_j') \\
&\quad = Obj(r_0') \\
&\qquad \wedge (Q(r_0') \cap Q(r_1') \cap H \neq \emptyset) \\
&\qquad \ldots \\
&\qquad \wedge (Q(r_{j-1}') \cap Q(r_j') \cap H \neq \emptyset)
\end{aligned}
$$

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:

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

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 the Byzantine majority algorithm 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.

$$
\begin{aligned}
P &= H \cup F \\
H \cap F &= \emptyset
\end{aligned}
$$

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:

$$
\begin{aligned}
&|Q(r_1') \cap Q(r_2')| = \\
&\quad |Q(r_1')| + |Q(r_2')| \\
&\quad - |Q(r_1') \cup Q(r_2')| \\
&\quad \geq (2f + 1) + (2f + 1) \\
&\quad - (3f + 1) \\
&= f + 1
\end{aligned}
$$

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

$$
\begin{aligned}
&|Q(r_1') \cap Q(r_2')| \\
&\quad = |Q(r_1') \cap Q(r_2') \cap H| \\
&\quad + |Q(r_1') \cap Q(r_2') \cap F| \\
&Q(r_1') \cap Q(r_2') \cap H| \\
&\quad = |Q(r_1') \cap Q(r_2')| \\
&\quad - |Q(r_1') \cap Q(r_2') \cap F| \\
&f \geq |Q(r_1') \cap Q(r_2') \cap F| \\
&|Q(r_1') \cap Q(r_2') \cap H| \geq f + 1 - f = 1
\end{aligned}
$$

□

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:

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

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

□

Now that we have described the Byzantine majority algorithm as a lossless expert model, we can now imagine how we might approximate it.

2.2 Sampling

One simple approach to approximating the Byzantine majority which may spring to the mind of the statistician is to sample the quora of the Byzantine majority. That is, to pick at random from all possible quora and consider this in place of the Byzantine majority. As we will show, though this is trivial, it has appealing combinatorial properties.

Assume our sampling algorithm works 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 neither has 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 $\gamma = \frac{k}{f}$.

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

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 that the probability of rendering a decision $Pr[Accepted](f, k) \geq Pr[\mathcal{R}](f, k) + Pr[\mathcal{C}](f, k)$. 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 the Byzantine majority algorithm $\Theta(B_f)$. More specifically, we have that:

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

Via this naive sampling approach, we have already roughly halved the expected complexity of the Byzantine majority algorithm. 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:

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

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:

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

Substituting and rearranging, we can describe the lost on *Cor* term of the Byzantine majority algorithm due to sampling:

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

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 $Closs_{\mathcal{B}_{f,k}}(r'_j)$ which are comparable to cryptographic security standards can be achieved using only a fraction of the replicas. Replicas which are not involved may pre-compute elements of other state transitions, lending to horizontal scalability.

Consistency, as defined by the intersection of consecutive state transitions in an honest replica by *Cons*, 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 and later unify 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 the Byzantine majority algorithm that can be composed, as we have done in our resampling construction. Ultimately, these compositions may yield algorithms with subtle but potentially advantageous properties.

3 Byzantine Fault Allowance

The titular concept of Byzantine Fault Allowance can be thought of idiomatically as referring to a state machine replica protocol which may propagate state changes with some known probability. A BFA protocol thus intentionally "allows" Byzantine faults.

In Motivation, we noted several combinatorial properties which could be relaxed in order to increase the Byzantine fault allowance of a state machine replica protocol. We will now formalize these properties and develop the class BFA.

3.1 Template Styles

The primary parameter given to the "`acmart`" document class is the *template style* which corresponds to the kind of publication or SIG publishing the work. This parameter is enclosed in square brackets and is a part of the `documentclass` command:

```
\documentclass[STYLE]{acmart}
```

Journals use one of three template styles. All but three ACM journals use the `acmsmall` template style:

- `acmsmall`: The default journal template style.
- `acmlarge`: Used by JOCCH and TAP.
- `acmtog`: Used by TOG.

The majority of conference proceedings documentation will use the `acmconf` template style.

- `sigconf`: The default proceedings template style.
- `sigchi`: Used for SIGCHI conference articles.
- `sigplan`: Used for SIGPLAN conference articles.

3.2 Template Parameters

In addition to specifying the *template style* to be used in formatting your work, there are a number of *template parameters* which modify some part of the applied template style. A complete list of these parameters can be found in the *LaTeX User's Guide.*

Frequently-used parameters, or combinations of parameters, include:

- `anonymous,review`: Suitable for a "double-anonymous" conference submission. Anonymizes the work and includes line numbers. Use with the `\acmSubmissionID` command to print the submission's unique ID on each page of the work.
- `authorversion`: Produces a version of the work suitable for posting by the author.
- `screen`: Produces colored hyperlinks.

This document uses the following string as the first command in the source file:

```
\documentclass[manuscript,screen,review]{acmart}
```

4 Modifications

Modifying the template — including but not limited to: adjusting margins, typeface sizes, line spacing, paragraph and list definitions, and the use of the `\vspace` command to manually adjust the vertical spacing between elements of your work — is not allowed.

Your document will be returned to you for revision if modifications are discovered.

5 Typefaces

The "`acmart`" document class requires the use of the "Libertine" typeface family. Your TeX installation should include this set of packages. Please do not substitute other typefaces. The "`lmodern`" and "`ltimes`" packages should not be used, as they will override the built-in typeface families.

6 Title Information

The title of your work should use capital letters appropriately - https://capitalizemytitle.com/ has useful rules for capitalization. Use the `title` command to define the title of your work. If your work has a subtitle, define it with the `subtitle` command. Do not insert line breaks in your title.

If your title is lengthy, you must define a short version to be used in the page headers, to prevent overlapping text. The `title` command has a "short title" parameter:

```
\title[short title]{full title}
```

7 Authors and Affiliations

Each author must be defined separately for accurate metadata identification. As an exception, multiple authors may share one affiliation. Authors' names should not be abbreviated; use full first names wherever possible. Include authors' e-mail addresses whenever possible.

Grouping authors' names or e-mail addresses, or providing an "e-mail alias," as shown below, is not acceptable:

```
\author{Brooke Aster, David Mehldau}
\email{dave,judy,steve@university.edu}
\email{firstname.lastname@phillips.org}
```

The `authornote` and `authornotemark` commands allow a note to apply to multiple authors — for example, if the first two authors of an article contributed equally to the work.

If your author list is lengthy, you must define a shortened version of the list of authors to be used in the page headers, to prevent overlapping text. The following command should be placed just after the last `\author{}` definition:

```
\renewcommand{\shortauthors}{McCartney, et al.}
```

Omitting this command will force the use of a concatenated list of all of the authors' names, which may result in overlapping text in the page headers.

The article template's documentation, available at https://www.acm.org/publications/proceedings-template, has a complete explanation of these commands and tips for their effective use.

Note that authors' addresses are mandatory for journal articles.

8 Rights Information

Authors of any work published by ACM will need to complete a rights form. Depending on the kind of work, and the rights management choice made by the author, this may be copyright transfer, permission, license, or an OA (open access) agreement.

Regardless of the rights management choice, the author will receive a copy of the completed rights form once it has been submitted. This form contains LaTeX commands that must be copied into the source document. When the document source is compiled, these commands and their parameters add formatted text to several areas of the final document:

- the "ACM Reference Format" text on the first page.
- the "rights management" text on the first page.
- the conference information in the page header(s).

Rights information is unique to the work; if you are preparing several works for an event, make sure to use the correct set of commands with each of the works.

The ACM Reference Format text is required for all articles over one page in length, and is optional for one-page articles (abstracts).

9 CCS Concepts and User-Defined Keywords

Two elements of the "acmart" document class provide powerful taxonomic tools for you to help readers find your work in an online search.

The ACM Computing Classification System — https://www.acm.org/publications/class-2012 — is a set of classifiers and concepts that describe the computing discipline. Authors can select entries from this classification system, via https://dl.acm.org/ccs/ccs.cfm, and generate the commands to be included in the LaTeX source.

User-defined keywords are a comma-separated list of words and phrases of the authors' choosing, providing a more flexible way of describing the research being presented.

CCS concepts and user-defined keywords are required for for all articles over two pages in length, and are optional for one- and two-page articles (or abstracts).

10 Sectioning Commands

Your work should use standard LaTeX sectioning commands: `\section`, `\subsection`, `\subsubsection`, `\paragraph`, and `\subparagraph`. The sectioning levels up to `\subsubsection` should be numbered; do not remove the numbering from the commands.

Simulating a sectioning command by setting the first word or words of a paragraph in boldface or italicized text is **not allowed.**

Below are examples of sectioning commands.

10.1 Subsection

This is a subsection.

10.1.1 Subsubsection. This is a subsubsection.

Table 1: Frequency of Special Characters

Non-English or Math	Frequency	Comments
Ø	1 in 1,000	For Swedish names
π	1 in 5	Common in math
\$	4 in 5	Used in business
Ψ_1^2	1 in 40,000	Unexplained usage

Paragraph. This is a paragraph.

Subparagraph This is a subparagraph.

11 Tables

The "`acmart`" document class includes the "`booktabs`" package — https://ctan.org/pkg/booktabs — for preparing high-quality tables.

Table captions are placed *above* the table.

Because tables cannot be split across pages, the best placement for them is typically the top of the page nearest their initial cite. To ensure this proper "floating" placement of tables, use the environment **table** to enclose the table's contents and the table caption. The contents of the table itself must go in the **tabular** environment, to be aligned properly in rows and columns, with the desired horizontal and vertical rules. Again, detailed instructions on **tabular** material are found in the *LaTeX User's Guide*.

Immediately following this sentence is the point at which Table 1 is included in the input file; compare the placement of the table here with the table in the printed output of this document.

To set a wider table, which takes up the whole width of the page's live area, use the environment **table*** to enclose the table's contents and the table caption. As with a single-column table, this wide table will "float" to a location deemed more desirable. Immediately following this sentence is the point at which Table 2 is included in the input file; again, it is instructive to compare the placement of the table here with the table in the printed output of this document.

Always use midrule to separate table header rows from data rows, and use it only for this purpose. This enables assistive technologies to recognise table headers and support their users in navigating tables more easily.

12 Math Equations

You may want to display math equations in three distinct styles: inline, numbered or non-numbered display. Each of the three are discussed in the next sections.

12.1 Inline (In-text) Equations

A formula that appears in the running text is called an inline or in-text formula. It is produced by the **math** environment, which can be invoked with the usual `\begin ...\end` construction or with the short form `$ ...$`. You can use any of the symbols and structures, from α to ω, available in LaTeX [?]; this section will simply show a few examples of in-text equations in context. Notice how this equation: $\lim_{n\rightarrow \infty} x = 0$,

Table 2: Some Typical Commands

Command	A Number	Comments
`\author`	100	Author
`\table`	300	For tables
`\table*`	400	For wider tables

set here in in-line math style, looks slightly different when set in display style. (See next section).

12.2 Display Equations

A numbered display equation—one set off by vertical space from the text and centered horizontally—is produced by the **equation** environment. An unnumbered display equation is produced by the **displaymath** environment.

Again, in either environment, you can use any of the symbols and structures available in LaTeX; this section will just give a couple of examples of display equations in context. First, consider the equation, shown as an inline equation above:

$$\lim_{n\rightarrow\infty}x=0 \tag{1}$$

Notice how it is formatted somewhat differently in the **displaymath** environment. Now, we'll enter an unnumbered equation:

$$\sum_{i=0}^{\infty} x + 1$$

and follow it with another numbered equation:

$$\sum_{i=0}^{\infty}x_i=\int_{0}^{\pi+2} f \tag{2}$$

just to demonstrate LaTeX's able handling of numbering.

13 Figures

The "`figure`" environment should be used for figures. One or more images can be placed within a figure. If your figure contains third-party material, you must clearly identify it as such, as shown in the example below.

Your figures should contain a caption which describes the figure to the reader.

Figure captions are placed *below* the figure.

Every figure should also have a figure description unless it is purely decorative. These descriptions convey what's in the image to someone who cannot see it. They are also used by search engine crawlers for indexing images, and when images cannot be loaded.

A figure description must be unformatted plain text less than 2000 characters long (including spaces). **Figure descriptions should not repeat the figure caption – their purpose is to capture important information that is not already provided in the caption or the main text of the paper.** For figures that convey important and complex new information, a short text description may not be adequate. More complex alternative descriptions can be placed in an appendix and referenced in a short figure description.

Figure 1: 1907 Franklin Model D roadster. Photograph by Harris & Ewing, Inc. [Public domain], via Wikimedia Commons. (https://goo.gl/VLCRBB).

For example, provide a data table capturing the information in a bar chart, or a structured list representing a graph. For additional information regarding how best to write figure descriptions and why doing this is so important, please see https://www.acm.org/publications/taps/describing-figures/.

13.1 The "Teaser Figure"

A "teaser figure" is an image, or set of images in one figure, that are placed after all author and affiliation information, and before the body of the article, spanning the page. If you wish to have such a figure in your article, place the command immediately before the `\maketitle` command:

```
\begin{teaserfigure}
  \includegraphics[width=\textwidth]{sampleteaser}
  \caption{figure caption}
  \Description{figure description}
\end{teaserfigure}
```

14 Citations and Bibliographies

The use of BibTeX for the preparation and formatting of one's references is strongly recommended. Authors' names should be complete — use full first names ("Donald E. Knuth") not initials ("D. E. Knuth") — and the salient identifying features of a reference should be included: title, year, volume, number, pages, article DOI, etc.

The bibliography is included in your source document with these two commands, placed just before the `\end{document}` command:

```
\bibliographystyle{ACM-Reference-Format}
\bibliography{bibfile}
```

where "`bibfile`" is the name, without the "`.bib`" suffix, of the BibTEX file.

Citations and references are numbered by default. A small number of ACM publications have citations and references formatted in the "author year" style; for these exceptions, please include this command in the **preamble** (before the command "`\begin{document}`") of your LATEX source:

```
\citestyle{acmauthoryear}
```

Some examples. A paginated journal article [**?**], an enumerated journal article [**?**], a reference to an entire issue [**?**], a monograph (whole book) [**?**], a monograph/whole book in a series (see 2a in spec. document) [**?**], a divisible-book such as an anthology or compilation [**?**] followed by the same example, however we only output the series if the volume number is given [**?**] (so Editor00a's series should NOT be present since it has no vol. no.), a chapter in a divisible book [**?**], a chapter in a divisible book in a series [**?**], a multi-volume work as book [**?**], a couple of articles in a proceedings (of a conference, symposium, workshop for example) (paginated proceedings article) [**? ?**], a proceedings article with all possible elements [**?**], an example of an enumerated proceedings article [**?**], an informally published work [**?**], a couple of preprints [**? ?**], a doctoral dissertation [**?**], a master's thesis: [**?**], an online document / world wide web resource [**? ? ?**], a video game (Case 1) [**?**] and (Case 2) [**?**] and [**?**] and (Case 3) a patent [**?**], work accepted for publication [**?**], 'YYYYb'-test for prolific author [**?**] and [**?**]. Other cites might contain 'duplicate' DOI and URLs (some SIAM articles) [**?**]. Boris / Barbara Beeton: multi-volume works as books [**?**] and [**?**]. A presentation [**?**]. An article under review [**?**]. A couple of citations with DOIs: [**? ?**]. Online citations: [**? ? ?**]. Artifacts: [**?**] and [**?**].

15 Acknowledgments

Identification of funding sources and other support, and thanks to individuals and groups that assisted in the research and the preparation of the work should be included in an acknowledgment section, which is placed just before the reference section in your document.

This section has a special environment:

```
\begin{acks}
...
\end{acks}
```

so that the information contained therein can be more easily collected during the article metadata extraction phase, and to ensure consistency in the spelling of the section heading.

Authors should not prepare this section as a numbered or unnumbered `\section`; please use the "`acks`" environment.

16 Appendices

If your work needs an appendix, add it before the "`\end{document}`" command at the conclusion of your source document.

Start the appendix with the "`appendix`" command:

```
\appendix
```

and note that in the appendix, sections are lettered, not numbered. This document has two appendices, demonstrating the section and subsection identification method.

17 Multi-language papers

Papers may be written in languages other than English or include titles, subtitles, keywords and abstracts in different languages (as a rule, a paper in a language other than English should include an English title and an English abstract). Use `language=...` for every language used in the paper. The last language indicated is the main language of the paper. For example, a French paper with additional titles and abstracts in English and German may start with the following command

```
\documentclass[sigconf, language=english, language=german,
                language=french]{acmart}
```

The title, subtitle, keywords and abstract will be typeset in the main language of the paper. The commands `\translatedXXX`, `XXX` begin title, subtitle and keywords, can be used to set these elements in the other languages. The environment `translatedabstract` is used to set the translation of the abstract. These commands and environment have a mandatory first argument: the language of the second argument. See `sample-sigconf-i13n.tex` file for examples of their usage.

18 SIGCHI Extended Abstracts

The "`sigchi-a`" template style (available only in LATEX and not in Word) produces a landscape-orientation formatted article, with a wide left margin. Three environments are available for use with the "`sigchi-a`" template style, and produce formatted output in the margin:

`sidebar`: Place formatted text in the margin.
`marginfigure`: Place a figure in the margin.
`margintable`: Place a table in the margin.

Acknowledgments

To Robert, for the bagels and explaining CMYK and color spaces.

A Research Methods

A.1 Part One

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi malesuada, quam in pulvinar varius, metus nunc fermentum urna, id sollicitudin purus odio sit amet enim. Aliquam ullamcorper eu ipsum vel mollis. Curabitur quis dictum nisl. Phasellus vel semper risus, et lacinia dolor. Integer ultricies commodo sem nec semper.

A.2 Part Two

Etiam commodo feugiat nisl pulvinar pellentesque. Etiam auctor sodales ligula, non varius nibh pulvinar semper. Suspendisse nec lectus non ipsum convallis congue hendrerit vitae sapien. Donec at laoreet eros. Vivamus non purus placerat, scelerisque diam eu, cursus ante. Etiam aliquam tortor auctor efficitur mattis.

B Online Resources

Nam id fermentum dui. Suspendisse sagittis tortor a nulla mollis, in pulvinar ex pretium. Sed interdum orci quis metus euismod, et sagittis enim maximus. Vestibulum gravida massa ut felis suscipit congue. Quisque mattis elit a risus ultrices commodo venenatis eget dui. Etiam sagittis eleifend elementum.

Nam interdum magna at lectus dignissim, ac dignissim lorem rhoncus. Maecenas eu arcu ac neque placerat aliquam. Nunc pulvinar massa et mattis lacinia.

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009