Partial Replay of Long-Running Applications

Alvin Cheung, Armando Solar-Lezama, and Samuel Madden
MIT CSAIL
{akcheung, asolar, madden}@csail.mit.edu

ABSTRACT

Bugs in deployed software can be extremely difficult to track down. Invasive logging techniques, such as logging all non-deterministic inputs, can incur substantial runtime overheads. This paper shows how symbolic analysis can be used to re-create path equivalent executions for very long running programs such as databases and web servers. The goal is to help developers debug such long-running programs by allowing them to walk through an execution of the last few requests or transactions leading up to an error. The challenge is to provide this functionality without the high runtime overheads associated with traditional replay techniques based on input logging or memory snapshots. Our approach achieves this by recording a small amount of information about program execution, such as the direction of branches taken, and then using symbolic analysis to reconstruct the execution of the last few inputs processed by the application, as well as the state of memory before these inputs were executed.

We implemented our technique in a new tool called bbr. In this paper, we show that it can be used to replay bugs in long-running single-threaded programs starting from the middle of an execution. We show that bbr incurs low recording overhead (avg. of 10%) during program execution, which is much less than existing replay schemes. We also show that it can reproduce real bugs from web servers, database systems, and other common utilities.

Categories and Subject Descriptors
D.2.5 [Software Engineering] – Testing and Debugging

General Terms Reliability, Performance

1. INTRODUCTION

A large amount of research effort has been devoted to the problem of identifying bugs and helping programmers pinpoint their root causes. However, not all bugs are equal. Most development organizations already have more bug reports than resources to fix them. As such, a bug from an important customer is much more critical than a bug discovered by an automated test generator. Unfortunately, pinpointing and fixing such critical bugs in the field can be very challenging. Stack traces and core dumps can be helpful when dealing with some errors, and statistical bug isolation can be used when a bug affects large numbers of users. However, for bugs only manifest as a result of a specific input, these techniques are not useful.

The gold standard for pinpointing such bugs is program replay. If users could provide a log of the entire execution of their system or all of its inputs, then identifying and fixing such bugs would be simple: when the bug is observed, you would have a complete trace of the execution that could be used to reproduce and fix the bug. In fact, replay tools exist that are able to reconstruct an execution by either taking periodic snapshots of the system state [33], or by logging all non-deterministic inputs to the target program, such as the return values from non-deterministic functions (e.g., random), system calls, and user inputs [17]. The problem with these tools, however, is that while they can reproduce the exact scenario that leads to the buggy behavior (modulo hardware failures), they can significantly slow down the normal execution of the program and produce very large data logs that may grow without bound as long as the program keeps executing. This makes them impractical for debugging systems like databases and web servers that may run for months at a time.

To mitigate this runtime overhead problem, there has been work done on performing software replay using symbolic execution [31, 15, 19]. The idea is to capture a subset of the program state during runtime, thus incurring less overhead, and then use symbolic execution to reconstruct the missing information. Even though the reconstructed state might not be exactly the same as the one that the user experienced, it is nonetheless useful for debugging purposes, since it is usually the case that the same bug can be triggered by multiple execution traces. Thus, as long as the reconstructed trace can still trigger the bug then it is good enough. Unfortunately, all the previous work focuses on replaying programs from the beginning of the execution, and today’s symbolic execution engines (which rely on SMT solvers) are not able to replay programs that have been running for days or months.

In this paper, we explore the idea of using symbolic execution to perform partial replay from the middle of executions, rather than replaying long-running programs from the very beginning. By doing this, we avoid having to store and transmit very large logs (as required by deterministic replacers) and mitigate the very long replay times that can result from symbolic execution. Our tool, called bbr, is the first
such partial symbolic replay tool. To use bbr, the developer annotates the code with checkpoints, for instance at places in the program that mark the transition from processing one request or phase to the next, such as at each invocation of the query parser in a database server. bbr collects a log during program execution and, when a checkpoint is reached, discards all logged data that was previously collected, limiting the size of the logs that need to be maintained. When the program terminates, the developer gives the (partial) log to bbr to replay starting from the last checkpoint. bbr symbolically executes the program, generating constraints when the program uses values that were not recorded. At the end of the symbolic execution, the constraints are solved to find the program state at the beginning of the replay. The solved state might not be exactly the same as the one in the original execution, but it is one guaranteed to take the same control flow path when executed with the logged data. We refer to this as a branch-deterministic replay, and we show that such a replay is as useful as a fully deterministic replay in debugging a number of real-world bugs, while avoiding the expensive cost of the data-logging approaches.

Unlike the data-logging based schemes, bbr works by recording control flow (one bit per branch) and accessed array indices into a log during program execution, as well the current stack and file offset information for the currently opened files. When a checkpoint is taken. This amounts to much less data than in the data-log based approaches (which can accumulate large logs even in partial replay scenarios).

In summary, this paper makes the following contributions:

- We introduce the idea of partial symbolic replay at an arbitrary program point in the target application, which lets users replay long-running programs without the burden of maintaining large logs. Furthermore, we develop an algorithm to handle pointer aliases that arise during partial replay without using the theory of bit-vector arrays, which, as our results show, gives poor performance.

- We propose the concept of branch-deterministic replay by recording control flow and non-constant array indices, and demonstrate its applicability to data-intensive applications, showing low runtime overhead and small log sizes as compared to other existing replacers.

- We identify several techniques that enable replaying of real-world applications in our bbr prototype, including a new memory model, separating constraints into independent subgroups during solving, and building a parallel solver implementation.

- We show that our technique can scale to replay real programs, including sqlite running on a 10 GB TPC-C database and two different web servers. Our runtime overheads range from 1% to 33%, with reasonable replay and solving times. We also show that we can reproduce several real bugs in these systems.

The rest of this paper is organized as follows. In Section 2, we overview the architecture of bbr and provide a sample usage scenario. In Section 3, we discuss in detail the design of the different components of bbr. Section 4 describes our experimental evaluation of bbr on a number of different real-world applications. Finally, Section 5 surveys related work, followed by conclusions in Section 6.

2. OVERVIEW

bbr consists of five components: a bytecode compiler, a library for the instrumentation routines, a bytecode replayer, a parallel solver, and a debugger. Fig. 1 shows the steps involved in using bbr for replay.

We illustrate the operation of these components through a real-world bug in memcached. In version 1.2.6, a bug was found in decrementing an existing value in the cache. The (slightly abridged) code is as follows:

```
char *do_add_delta (item *it, const int64_t delta) {
    int64_t value = ITEM_data(it);
    if (incr) {
        value += delta;
        MEMCACHED_COMMAND_INCR(ITEM_key(it), value);
    } else {
        value -= delta;
        if(value < 0) {
            value = 0;
            MEMCACHED_COMMAND_DECR(ITEM_key(it), value);
        }
    }
}
```

The function first obtains the existing value for a key from the cache at line 2622 before performing the decrement. Then, if the resulting value is negative, the code simply sets the new value to be 0. This is a bug since value is treated as a signed entity, contrary to memcached’s specifications. If the existing value is a large number with the most significant bit set, then decrementing it will result in 0. In the following, we describe how a developer can use bbr to replay and debug this problem.

2.1 Preparing for Replay

To use bbr, the developer first prepares the source code by inserting the bbr checkpoint annotations. The annotation can be inserted in two ways: at a program point for which the developer would like to start replay from (e.g., at the point that processes each incoming requests), or configured as a timing parameter (e.g., take a checkpoint every five minutes). In our example, the developer can put the annotation at the program point that calls different functions (e.g., do_add_delta) based on the incoming request type.
The developer then uses the bbr compiler to compile the code into LLVM bytecode. The bbr compiler links the user code with a modified version of the uClibc [2] library (which we use because it can be easily compiled into LLVM bytecode). During compilation, the compiler inserts instrumentation routines to record two types of data. First, bbr records the values of conditional branches, in the example the branch conditions at lines 2631 and 2636. Next, bbr records the values of non-constant indices into arrays (none in this case). The instrumented code is then compiled to native assembly and linked with the bbr instrumentation library to produce the final native memcached distribution.

2.2 Runtime Monitoring

The user starts using the instrumented memcached server in her application. As the application issues operations against the memcached server, the bbr library embedded in the server intercepts the branch outcomes and array indices from the running program and stores them in an in-memory buffer, which is periodically flushed to disk when it becomes full. When the checkpoint annotation is hit, the library takes a lightweight snapshot of the running program. It also discards any logs that are previously written to disk. In our example, the user has been running her application normally until one day she observes that memcached returns 0 for a decrement and causes her application to return an incorrect result. Believing that it is a problem in the server, she files a report to the memcached developer along with the log generated by bbr.

2.3 Symbolic Replay

The developer would like to find out why 0 was returned in the decrement operation, which is not obvious by just looking at the code. With the collected log and the instrumented bytecode, the developer uses the bbr replayer to replay. The replayer symbolically executes the bytecode from the last checkpoint. In our example, at line 2622, ITEM_data loads the data from the heap pointed to by it, whose contents are unknown since it was stored prior to the checkpoint. When that happens, the replayer creates a fresh symbolic variable v to represent the contents at the memory pointed to by it and assign that to value. At the branch point in line 2631, the replayer reads the branch log and finds that the branch was not taken, and jumps to line 2634. At line 2635, value is assigned to be v − d, where the symbolic variable d represents the value of the program variable delta. Finally, at line 2636, from the branch log the replayer learns that the branch was taken, and because the branching condition involves symbolic variables, it generates the constraint v − d < 0 and continues execution.

2.4 Solving and Debugging

The replayer saves the generated constraints to a file at the end of the replay, which are then given to the bbr parallel solver to solve. In our example, the solver solves for possible values of v and d in order to produce a branch-deterministic execution from the last checkpoint. Suppose the solver returns $2^{63} + 1$ for $v$, and 1 and 1 for $d$. To map these results back to the program, bbr comes with a debugger. The debugger allows the developer to specify the values to be printed when an instruction is reached during symbolic execution. A sample session is as follows (italic text represents user inputs):

```
$ bbr-db> print delta at 2622; print value at 2622;
bbr-db> run
at 2622: delta = 1
at 2622: value = 9223372036854775809 // 2^{63} + 1
```

With the output above and by following the program logic, the developer realizes the cause of the bug, and fixes her code accordingly. Even though the solved values might not be exactly the same as those that the user originally saw (in fact, the insertion of the key into the cache could have happened a long time ago with a different value in the original execution), the developer is still able to use bbr to diagnose the problem by finding an execution that leads to the behavior observed by the user.

The debugger also allows the developer to request a new feasible variable assignment if she isn’t satisfied with a given assignment by appending extra constraints. In the example above, perhaps the developer knows that the value of delta was not 1, and thus the solution does not represent a feasible program state. In that case, she can tell the debugger that delta does not equal to 1, and ask the debugger to generate another set of values for delta and value.

In contrast, in order to use existing tools to replay the bug, the developer would either have to rely on the user to provide a detailed use case that illustrates the bug, or to collect data logs that have recorded the values of all nondeterministic data since memcached started (which could have been a long time ago), or to write assertions and rely on test generators to hit upon the bug, all of which are costly and error-prone.

In the next section, we discuss the details of the design of the bbr replayer.

3. BBR DESIGN

We begin by explaining the implementation of the recording mechanism, followed by that of the replayer and parallel constraint solver.

3.1 Instrumentation for Recording

As discussed in Section 2, calls to the instrumentation functions are added to the user code during compilation with the bbr compiler to collect the necessary data for replay. These functions are implemented in a separate library that is linked with the instrumented assembly when producing the native executable. Each conditional branch generates 1 bit of data, and other types of data (such as array indices) are 4 bytes each. To reduce disk overhead, we use a double-buffering mechanism where we log data in one buffer in memory. When the buffer fills (or the program terminates), we flush it to disk in the background and start recording into the other buffer. Section 3.2.4 reports the overhead of data collection. When a checkpoint annotation is reached, bbr records the current stack and the state of open files (see Section 4.1 for details) so that replay can start at the appropriate program point. The contents of registers and heap memory are not saved, making the operation very fast.

3.2 Replayer Design

Once data logs are collected, the developer feeds them to the replayer, which uses them to generate the constraints used to solve for inputs and program state consistent with the log. Using the branch log, the stream of bytecode instructions (Fig. 2) in the original execution is reconstructed,
Program always statically known in such cases.

to change only

This approach is that we assume pointer arithmetic to be able alias map

symbolic values currently assigned to them, as well as an

tains an environment

programs and to reproduce real bugs that are often much

Exchange for this, we are able to scale to large, long-running

array element access instructions.

l, n

produced by malloc

to leverage the concrete information we have rather than

before the start of replay, and the key to our approach is

the execution. In our system, we know the addresses for all

cient because the solver doesn’t have to reason about alias-

puts too much strain on the SMT solver [35]. At the other

modeling memory as a giant array that gets updated with

way to model memory has been by using the theory of arrays,

replayer is memory representation. Traditionally, the easiest

concrete reasoning, and has implications for the design of

tradeoffs in terms of how much we can rely on symbolic vs.

itself, we get it from the log. This subtle difference requires

that instead of getting our concrete data from the execution

n

Figure 2: Language of bytecode instructions

and instructions are emulated to generate constraints. The

constraint generation process mirrors the symbolic execution
done in concolic analysis (e.g., [32]); the main difference is

that instead of getting our concrete data from the execution
itself, we get it from the log. This subtle difference requires

tradeoffs in terms of how much we can rely on symbolic vs.

concrete reasoning, and has implications for the design of

the symbolic state and constraint generation.

3.2.1 Modeling State

The most interesting aspect of the state maintained by the

replayer is memory representation. Traditionally, the easiest

way to model memory has been by using the theory of arrays,

modeling memory as a giant array that gets updated with

every write operation. This approach is very general, but

puts too much strain on the SMT solver [35]. At the other

extreme, if we know the concrete address of every load and

store, we can model the heap as a map that gets modified by

read and write operations [32, 33, 34, 35]. This is very effi-
cient because the solver doesn’t have to reason about alias-
ing, but it also requires a lot of concrete knowledge about

the execution. In our system, we know the addresses for all

memory accesses except those involving memory allocated

before the start of replay, and the key to our approach is

to leverage the concrete information we have rather than

relying on the theory of arrays to discover it.

The first important element of our representation is that

it models the heap as a collection of independent buffers

produced by malloc rather than as a flat array. In this view,

a pointer is a pair (l, n), where l is the base address of a

buffer assigned by malloc, and n is an offset into the buffer.

The benefit of this is that during runtime we only need to

record n and only when it is statically unknown in LLVM

array element access instructions.¹ The main downside of

this approach is that we assume pointer arithmetic to be able to

change only n but not l, which prevents the system from

reproducing errors caused by unsafe memory operations.

In exchange for this, we are able to scale to large, long-running

programs and to reproduce real bugs that are often much

closer to discover than memory errors (see Section 4.2).

In addition to the heap h : (l, n) → c, the replayer main-

tains an environment σ : r → e, that maps variables to the

symbolic values currently assigned to them, as well as an

alias map α : l → {l₀, . . . , lₜ} that stores may-alias locations

¹Field in records are accessed in the same way, however n is
always statically known in such cases.

cond b := true | false | ¬b | e₁ op e₂ | b₁ ∧ b₂ | b₁ ∨ b₂

stmt s := r = malloc n | r = ep | *r = ep | r = *ep | assert b

program p := s; p

n ∈ N, r ∈ {program variables}

(l, n) ∈ {memory locations}, unop ∈ {¬

binop ∈ {+, −, ∗, /, mod, band, bor, xor, shl, lshr, ashr}

comp ∈ {≤, ≥, <, ≤, ≠}

We denote a memory location as (l, n), where l represents an

allocation, and n is the offset from the base of allocation.

Figure 2: Language of bytecode instructions

for a given allocation l. Finally, b represents the set of con-

straints accumulated so far in the execution. Together, the

four entities (σ, h, b, a) make up the state of the replayer.

3.2.2 Symbolic Execution of Memory Operations

Our treatment of non-memory operations is similar to

standard symbolic execution [32], as illustrated by Fig. 3.

However, memory operations present new challenges. First

of all, a read or a write to an address (l, n) is easy to handle

if we know the concrete values of l and n, since we can just

read or update the corresponding entry in our model of the

heap. The challenge comes when we lack information about

an address as a consequence of partial replay. The reason

partial replay makes this difficult is because when we read

a location that was written to before the start of the log, we

know nothing about its contents, and if it contains an ad-

dress, we have no information about either l or n, or about

its aliasing relationship with other addresses.

Because of this, our system does not know the invariants

the non-replayed execution enforced on memory contents.

For the replayed portion of the program, bbr ensures that for

every location (l, n), and all its potentially aliased locations

(l₁, n₁), the following invariant is maintained:

SolverValue(l, n) = SolverValue(l₁, n₁) ⇒

SolverValue(h[l₁, c]) = SolverValue(h[l₁, c])

In other words, if the solver decides that ℓ₁ is actually aliased

to ℓ, then the symbolic expression in h[ℓ₁, c] should evaluate
to the same value as the symbolic expression in h[ℓ, c].

In the following, we show this invariant is preserved in

memory operations, and describe how we handle memory

locations initialized before the start of partial replay.

Address Initialization: Consider reading from or writing
to memory whose address is stored in variable variable

r. If σ[r] maps to some location (l, n), then the operation

proceeds as described below. Otherwise, r holds a value that

was written before the start of partial replay (i.e., σ[r] = ⊥).

When this happens, the system assigns a fresh symbolic vari-

able bv to represent r. Furthermore, it assigns bv a brand

new base address ℓ, that is different from all the ℓ’s currently

in use by the program, updates σ[r → (ℓ, 0)], and generates

the constraint bv = (ℓ, 0). To account for the possibility of

aliasing, the system updates the alias map a to keep track of

all the other ℓ’s that may be aliased with ℓ. Our current

implementation assumes that two memory locations can be

aliased to each other only if the program variables for which

they were originally allocated have the same static type,

and that a memory location cannot be aliased to some off-

set within another location (e.g., array variables a and b can

be aliased to each other, but a cannot be aliased to the ad-

resses of h[1], h[2], etc, and vice versa). Notice that this

is just one possible mechanism for computing alias informa-
tion, which we chose as it proved sufficient for replaying a

Figure 3: Semantics for non-memory instructions

\[ [r = \text{malloc}(n)](\sigma, h, b, a) = (\sigma[r \rightarrow (l, 0)], h, b, a[l \rightarrow {}]) \]

\[ [\text{assert } b_1](\sigma, h, b, a) = (\sigma, h, b \land b_1, a) \]
Memory Writes: Memory writes are processed according to the following rule:

$$\begin{align*}
\{ (l_i, c, True) \} &= \text{GetLoc}(\sigma[r]) \\
\{ (l_i, c, b_i) \} &= \text{GetLoc}(\sigma[r]) \\
\langle *r = e_c, (\sigma, h, b, a) \rangle &\rightarrow \langle \sigma, h', b, a \rangle
\end{align*}$$

This rule conditionally updates every address that is potentially aliased with the address stored in \( r \). The rule uses the function \( \text{GetLoc} \) to account for the fact that the address in \( r \) might itself have been the result of some conditional updates, so instead of a single address, \( \text{GetLoc} \) returns a guarded list of the possible addresses stored in \( \sigma[r] \). If \( \sigma[r] \) is a simple address \((l_e, c)\), \( \text{GetLoc}(\sigma[r]) \) returns \((l_e, c, True)\), but in general, \( \sigma[r] \) can be a complicated expression evaluating to different \((l_i, c_i)\) under different conditions \( b_i \). However, since we logged the value of the offsets, the rule can assume that those are fixed for all choices. For each memory location \((l_i, c)\) that is returned by \( \text{GetLoc} \), we store a conditional expression that evaluates to \( e_c \) only if \( *r \) does indeed evaluate to \((l_i, c)\); i.e., if \( b_i \) is true. For each memory location \( l_i \) that is aliased with each \( l_i \), we update \( h[(l_i, c)] \) to a conditional that reduces to \( e_c \) if \( b_i \) is indeed aliased to \( l_i \).

An important assumption in the rule above is that since we always know the offsets for memory accesses, we only have to track aliases among the base addresses. In the special case that an address is allocated with a call to \texttt{malloc} after the start of replay, there is no ambiguity as to what address is contained in a memory location, \( \text{GetLoc} \) simply returns one possible location for \( *r \), and that location has no aliases, so the rule simply reduces to standard heap update:

$$\begin{align*}
\{ (l_i, c, True) \} &= \text{GetLoc}(\sigma[r]) \\
\{ (l_i, c, b_i) \} &= \text{GetLoc}(\sigma[r]) \\
\langle *r = e_c, (\sigma, h, b, a) \rangle &\rightarrow \langle \sigma, h', b, a \rangle
\end{align*}$$

Memory Reads: Loading from memory presents similar complications and is processed using the following rule:

$$\begin{align*}
\{ (l_i, c, b_i) \} &= \text{GetLoc}(e_c) \\
\{ (l_i, c, b_i) \} &= \text{GetLoc}(e_c) \\
\langle \sigma = \sigma[r] \land \forall b_i. h[l_i(c_i)] \rangle &\rightarrow \langle \sigma', h, b, a \rangle
\end{align*}$$

The notation \( \forall b_i \rightarrow c_i \) above should be read as a switch statement that produces \( e_c \) if \( b_i \) is true. Note that we do not load from any of the may-alias locations of \( *e_c \) since the store rule above ensures that their values will be equivalent if the alias turns out to be real.

In summary, in the case where we have the log from the start of execution, our strategy for memory operations reduces to the very efficient modeling of memory as a map. Conversely, when we have no information about aliasing and all our locations are unknown, our strategy is just an inefficient implementation of the theory of arrays. For our purposes, however, this is ideal because it exploits all the concrete information available with the system, and allows us to deal with aliasing uncertainty while still exploiting any aliasing information that we can provide.

### 3.2.3 External Function Calls

A common issue in the symbolic execution of real-world programs is handling external functions such as libc and system calls. The typical solution, and the one we follow, is to provide a model of those functions. \( bbr \) follows the approach used in Klee [18] by linking a modified version of the uClibc library with the target program, which greatly reduces the number of libc functions that we need to model. We model a subset of system calls using bit vector values. For instance, we use a 4 byte bit vector to model the user ID of the calling process. Thus calls to \texttt{getuid} will return that bit vector. We currently model over 100 Linux system calls but do not model the state of devices or the kernel.

#### 3.2.4 File Descriptors and Network Sockets

\( bbr \) implements a simple symbolic file system where each file is modeled as follows:

- An array of symbolic expressions, where each entry in the array represents one byte in the file.
- A 4 byte integer for the current file offset.
- A 4 byte integer representing the file flags (read / write / both, and append / overwrite mode).
- A 4 byte integer representing the file permissions.
- A 4 byte integer representing the file size.

The file descriptor itself is modeled as a 4 byte bit vector variable, and the file system is a map from the file descriptors to the structure listed above. \( bbr \) currently supports typical file system calls, and network sockets are modeled similarly, except that they are append-only and do not support seek.

Because the file metadata are modeled as real integers (rather than bit vectors), \( bbr \) records values from file system operations (as mentioned in Section 2) in order to maintain each file’s internal state during symbolic execution. For instance, the return values from \texttt{read} calls are recorded so that the current file offset can be correctly updated.

We experimented with using bit vectors and the theory of arrays to represent the file contents, but this did not scale, while the approach above did. This is because the programs we experimented with operate on large files, but do not necessarily process each byte within those files (e.g., databases may only read a few tuples from a loaded page). Modeling these files with the theory of arrays caused a large number of bit vector variables to be created for indices that are not referenced. Our approach, which records additional information during runtime (4 bytes per each invocation of \texttt{read}, \texttt{write}, \texttt{lseek}, etc), allows us to implement our own file model that generates less complicated constraints, which saves a substantial amount of constraint solving time while adding relatively little additional recording state.

### 3.3 Soundness and Completeness

For partial replay, we define soundness as the fact that all program executions (i.e., the starting heap state and execution path) solved by the replayer are indeed feasible traces of the target program although not necessarily the same as the original execution, and completeness as the ability to solve for program executions given the input logs, provided that the inputs were from an actual execution.

\( bbr \) is unsound since the initial state of the heap generated at the beginning of the partial trace might not correspond to a feasible heap from the original program. This is because the system might miss some of the invariants that the non-recorded portion of the program enforces on...
the heap, so it might generate a heap that violates these
unstated invariants. On the other hand, bbr is incomplete
since we might not be able to replay executions that vi-
olate our assumptions, namely the independent allocation
and non-overlapping assumption, the memory alias assum-
ptions, and the fact that we do not model the hardware or
the kernel state. In practice, that means we cannot deter-
mine the memory locations that are overwritten in a buffer
overflow attack (although we can still detect writing out of
allocated boundaries errors), or replay an execution that is
caused by malfunctioning hardware.

### 3.4 Parallel Constraint Solver

Symbolic execution produces a set of constraints. The bit
vector variables in the constraints correspond to heap con-
tents before the start of replay, the non-deterministic inputs
that were read, as well as return values any external function
invocations during the execution. The constraints need to
be solved in order to re-create the values that would cause
the execution to take the same control flow path as in the
original run. A straight-forward implementation would send
all the generated constraints to a constraint solver to solve
in one bundle. We found, however, that this is quite slow as
the constraint sets can be very large.

Instead, we subdivide the constraints into independent
portions that can be solved separately. Specifically, we found
that although there are a large number of symbolic variables,
it is frequently the case that each variable is only related to
a handful of other variables. For instance, in replaying a
web server, each byte that is read from the incoming socket
is modeled as a bit vector variable as mentioned in Sec-

### 3.5 Using the output of the solver

The output of the solver is an assignment to each variable
involved in the constraints. bbr provides a debugger that
takes in the instrumented bytecode and the solved outputs.
Similar to the replayer, the debugger performs symbolic ex-

### 3.6 Experimental Evaluation

In this section, we describe our evaluation of the three
central claims of this paper:

- First, we compare the runtime overhead of bbr to other
  replay schemes. We measure both the overhead in
terms of slowdown to the running program and the
  size of the logs generated.

- Second, we evaluate bbr’s ability to help developers
  understand the vulnerable program state. Given a
  vulnerable program state, we run bbr and let the user
  debug the executed bytecode. The user can then
  execute the code and observe the new state.

- Third, we evaluate bbr’s performance on a range of
  benchmarks, including real-world applications and
  custom benchmarks.

We use the following benchmarks:

- Trivial benchmarks that are designed to test the
  basic functionality of bbr.

- Real-world applications that are designed to test the
  practical use of bbr.

- Custom benchmarks that are designed to test the
  performance of bbr.

We found that bbr is able to achieve a good balance
between performance and ease of use, and that it is able to
help developers understand and debug vulnerable programs
in a variety of settings.

### 4. Conclusions

In summary, we have presented bbr, a symbolic execution
framework that helps developers understand and debug
vulnerable programs. We have shown that bbr is able to
achieve a good balance between performance and ease of use,
and that it is able to help developers understand and debug
vulnerable programs in a variety of settings.
We ran 20k TPC-C transactions on top of a 10G database representing 10 warehouses and measured the time to complete all transactions. Checkpoints are taken every 10 transactions.

| memcached | We inserted or updated 10k keys into the cache, with values of size 800k each, and measured the time to complete all operations. Checkpoints are taken every 10 operations on the server. |
| tcpdump   | We asked tcpdump to print the details from a packet dump of 1G in size, and measured the time to process all the packets. Checkpoints are taken every 5 packets that are processed. |
| betaftpd  | We fetched 50 files from the server, each of size 1G, and measured the time to complete all operations. Checkpoints are taken every 5 fetching. |
| thttpd    | (same as betaftpd) |
| ghttpd    | (same as betaftpd) |

Figure 4: Description of benchmarks

- Next, we chose different types of bugs from real-world applications and examine bbr’s ability to replay them.
- Finally, we measure the effectiveness of the alias-aware memory model and constraint partitioning in bbr in replaying programs.

bbr is implemented with 11k LOC of C++ using LLVM version 2.6. We experimented with several different SMT solver implementations, but we only report numbers from those using Z3 [3] as that was the solver that we found to scale the best. For these experiments, replay was run on a 32-bit Ubuntu machine with 2GB of RAM, while the constraint solving was done on a 64-bit 4-core machine running Z3 version 2.14 on Windows Server 2003 with 24GB of RAM.

4.1 Overhead Experiments

In the first experiment, we measured the time and space overhead that different programs incur while collecting logs with periodic checkpoints. The programs we replayed are listed in Fig. 4. Fig. 5 shows the results of the time overhead experiment, in terms of slowdown relative to an uninstrumented binary, while Fig. 6 and Fig. 7 show the log sizes that were generated by the different recording schemes. All data collections were done using the bbr instrumentation library. We report the results from running five different versions of each application, namely:

- [Native]: Native uninstrumented version.
- [bbr]: bbr instrumented version with periodic checkpoints at frequencies shown in Fig. 4.
- [non-det]: Instrumented version that collects all non-deterministic data from the beginning of program execution. This models the overhead of a whole-program, fully deterministic replacer.
- [snapshot]: Same as non-det, except that every time a checkpoint annotation is reached, we fork a process to create a core dump, and all previously collected data are deleted. This models the overhead of a partial replacer that takes periodic snapshots of memory and logs non-deterministic inputs that were received between snapshots.
- [loads]: Instrumented version that records the values of all memory loads. To reduce the amount of logging,

we use the technique from iDNA [17] where we only record loads whose values are not predictable at runtime (i.e., the store to a location was not an explicit instruction in the application but rather a side-effect of a system call, such as storing to the buffer in `read`).

![Figure 5: Normalized execution time (relative to uninstrumented binary=1) for different applications, with uninstrumented times shown at bottom.](image)

![Figure 6: Log size experiment results](image)

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>bbr</th>
<th>non-det</th>
<th>snapshot</th>
<th>loads</th>
</tr>
</thead>
<tbody>
<tr>
<td>sqlite</td>
<td>7k</td>
<td>8G</td>
<td>1G</td>
<td>250M</td>
</tr>
<tr>
<td>memcached</td>
<td>16k</td>
<td>8G</td>
<td>600M</td>
<td>560M</td>
</tr>
<tr>
<td>tcpdump</td>
<td>3k</td>
<td>2.6G</td>
<td>1.8G</td>
<td>200M</td>
</tr>
<tr>
<td>betaftpd</td>
<td>72M</td>
<td>50G</td>
<td>5.1G</td>
<td>550M</td>
</tr>
<tr>
<td>thttpd</td>
<td>100M</td>
<td>50G</td>
<td>5.2G</td>
<td>300M</td>
</tr>
<tr>
<td>ghttpd</td>
<td>90M</td>
<td>50G</td>
<td>2.2G</td>
<td>2.2G</td>
</tr>
</tbody>
</table>
Table 7: Log growth rates in overhead experiment

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>bbr</th>
<th>non-det</th>
<th>snapshot</th>
<th>loads</th>
</tr>
</thead>
<tbody>
<tr>
<td>sqlite</td>
<td>1.4k/op</td>
<td>1M/op</td>
<td>0.2G/op</td>
<td>12.5k/op</td>
</tr>
<tr>
<td>memcached</td>
<td>1.6k/op</td>
<td>0.8M/op</td>
<td>0.1G/op</td>
<td>56.9k/op</td>
</tr>
<tr>
<td>tcpdump</td>
<td>0.6k/op</td>
<td>0.3M/op</td>
<td>0.1G/op</td>
<td>20k/op</td>
</tr>
<tr>
<td>betaftp</td>
<td>1.4M/op</td>
<td>1G/op</td>
<td>1G/op</td>
<td>55M/op</td>
</tr>
<tr>
<td>thttpd</td>
<td>20M/op</td>
<td>1G/op</td>
<td>1G/op</td>
<td>6M/op</td>
</tr>
<tr>
<td>ghhttp</td>
<td>19.8M/op</td>
<td>1G/op</td>
<td>1G/op</td>
<td>44M/op</td>
</tr>
</tbody>
</table>

Figure 7: Log growth rates in overhead experiment

<table>
<thead>
<tr>
<th># Requests</th>
<th>bbr</th>
<th>non-det</th>
<th>snapshot</th>
<th>loads</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>46M</td>
<td>10G</td>
<td>5.1G</td>
<td>47M</td>
</tr>
<tr>
<td>30</td>
<td>46M</td>
<td>30G</td>
<td>5.3G</td>
<td>150M</td>
</tr>
<tr>
<td>50</td>
<td>46M</td>
<td>50G</td>
<td>5.6G</td>
<td>300M</td>
</tr>
</tbody>
</table>

Figure 8: Log sizes with varying # of requests from bbr, since for some applications (such as sqlite and tcpdump), most of the values that are affected by system calls are indeed loaded by the application afterwards, for instance the read buffers in read and recv calls.

Since the number of operations stored in the various logs are not the same (e.g., bbr takes periodic checkpoints to reduce log sizes whereas non-det keeps the entire log from the beginning of execution), Fig. 7 presents the same results by showing the log growth rates instead. The results show that the bbr logs grow much slower as compared to others. Thus, even if the user decides to keep around all the bbr log files rather than having the system truncate them at each checkpoint (perhaps due to uncertainty as to which checkpoint the replay should start), bbr will still have the smallest log file sizes as compared to other schemes.

Next, we ran the experiment for betaftp, varying the number of requests issued in order to characterize the size of the data logs as the running time of the application increases (the results show that the execution overhead is relatively insensitive to the number of requests). The results are shown in Fig. 8. Observe that the log sizes for the non-det and loads schemes grow proportionally with execution time due to the lack of log truncation. And while the log sizes are roughly the same for bbr and snapshot, bbr incurs much less runtime overhead because it writes less data to disk, as shown in Fig. 7.

To understand how these numbers compare to other replay tools, we compared our time overheads to those reported for other replay tools on similar data-intensive programs. PRES reports an overhead of 43% when recording all basic blocks while running MySQL, and 1977% when recording PBZip2. R2 reports an overhead of 200% when logging all data from win32 system calls while running MySQL. iTarget reports a slowdown of nearly 400% on MySQL. Other tools designed to collect data during normal execution on different benchmarks report similar or larger overheads. For example, program shepherding reports up to 760% and dDNA reports an average of 1189%. In summary, the overheads of bbr are generally low enough (with an average of 10%) to be deployed as an online tool during normal program execution.

4.2 Reproducing Bugs

In our next experiment, we used bbr to replay different types of bugs from real-world programs. Fig. 9 shows the list of bugs that we tried to replay. We describe a few representative bugs in detail in Section 4.2.1 below.

We set up the applications in a similar way as in the overhead experiment, except that we input a request that would expose or trigger the bug. We then terminated the application (if it had not already terminated due to errors), and collected the logs. Given the log, we asked bbr to reproduce a plausible execution of the program from the last checkpoint. Fig. 10 shows some statistics about the bbr executions, specifically:

- LOC: Number of LLVM instructions emulated.
- # br: Number of conditional branch values recorded.
- [Replay]: Time taken for bbr’s symbolic execution.
- [Split]: Time taken to split the generated constraints into independent components.
- # constr: Total number of SMT constraints generated. Note that constraints that reduce to True are not included, thus the number of constraints can be smaller than number of conditional branches.
- # groups: Number of independent groups created.
- # vars: # of bit vector variables in the constraints.
- Solve: Time taken for parallel solving.
- Debug?: Whether the solved inputs can be used to identify the original bug.

These experiments show that bbr is able to symbolically execute a wide-range of real-world data-intensive applications and generate constraints that can be solved within a reasonable amount of time. Most of the replay time was spent in symbolic execution. Note that the number of conditional branch values recorded is typically much fewer than the number of constraints generated. That is because of peephole optimizations on the constraint expressions that bbr performs to eliminate constraints that reduces to True, and also because some of the conditional branches are not based on non-deterministic values in the program, so no constraints were generated.

4.2.1 Bug Walkthrough

Here we discuss a few bugs in detail. As discussed in Section 3.5, the decrement bug in memcached was caused by the incorrect treatment of the stored values as signed entities. Using bbr, we were able to solve for inputs and state of the value store that would trigger the problem. Notice that even though bbr did not record the contents of the request from the user, it was nonetheless able to reconstruct it given the branching decisions recorded during parsing of the request.

For the sqlite bugs, rather than a complete database file, the output of the solver is a combination of heap values and a partial database file that was read while processing the transactions since the last checkpoint. As described in Section 3.5, these outputs cannot be used directly to run sqlite and reproduce the bug, since the solved input file is incomplete. However, these solved values can still help developers debug. For instance, the collation bug was caused by an error in the implementation of the comparison operator between two expression trees, causing it to return the wrong cached value rather than performing the actual comparison. Using the solved values from the partial replay and the branch log, we were able to observe the error by tracking the solved values that were used as inputs to the comparison function, thanks to the bbr debugger. When invoked with those values, the function returns the incorrect value that triggers the bug.

For the bugs in tcpdump, bbr solved for the contents of the incoming packets that cause the infinite loops. While the contents were not exactly identical to the original ones, we have verified that they cause the same problems when fed into tcpdump.
In general, for all of the bugs that bbr was able to replay, even though the solved instances of the database contents / network packets / http requests / etc are not necessarily the exact same one as in the original input, they still exhibit the bugs. This illustrates the power of our approach – recording branches and a few extra pieces of data is enough for developers to debug the problem in hand. Also, observe that without using bbr’s partial replay ability, in order to replay these bugs it would be necessary to record all non-deterministic data from the beginning, or take periodic snapshots of the heap, which would be very costly as demonstrated. In both cases, there is a a huge overhead in both time and data log sizes. Furthermore, as our experiment shows, the longer the program runs, the worse the problem becomes.

bbr failed to replay the betaftpd non-Latin character bug. This is because the bug was caused by the lack of checking the characters that are read from the incoming socket before passing them to open. The constraints generated from symbolic execution simply bound the length of the file requested (since the code checks for ‘\0’), but not the contents that were read (this is precisely the reason why the bug exists). As a result, the solver returned a random filename that does not trigger the bug when re-executed. While the developer can use the bbr debugger to request another plausible value for the filename, it is unlikely that she will be able to hit upon one that causes the problem within a reasonable amount of time given the unconstrained nature of the bug. This illustrates a limitation of bbr – the ability to reconstruct a trace that leads to the problem relies on the fact that the buggy execution is sufficiently bound by the bbr logs. Otherwise, the solver might return a trace that does not trigger the error, even though it is branch-deterministic.

Finally, we note that for a few of these bugs (e.g., those from ghttpd), it is possible to replay them by just recording the incoming requests after the last checkpoint, since they do not involve the internal state of the program. However, it would be very difficult for a developer to know a priori whether the bugs that her program exhibits will involve the internal state of the application or not, unless the application keeps no internal state whatsoever, which is highly unlikely. For instance, the sqlite and memcached bugs are related to the internal state of the program (in particular, the cached values in memory). Thus, it would not be possible to replay such bugs simply by recording incoming requests.

### 4.3 Constraint Splitting
Next, we look at the effectiveness of splitting constraints into independent groups, using ghttpd and betaftpd as examples. We replayed different number of requests coming into the two servers and measured the solving time. We chose these two applications since they have relatively simple internal states, and each incoming request should be independent from each other in terms of the constraints that are generated. We compared the time taken to solve the generated constraints all at once from a single file (Single), and the total time needed to solve the split constraints, using 1000 threads for the parallel solver on a 4 core machine (Split).
4.4 Memory Model Implementation

Lastly, we looked at the performance differences between different memory models in our replay engine. As discussed in Section 3.2, bbr models memory as a conceptual mapping from program variables to constraint expressions. Internally, this is implemented using two maps, one that maps program variables to memory locations, and one that maps memory locations to contents in memory. There are different ways to implement the second map. We experimented with several different implementations for a 32-bit memory (i.e., addresses are 32-bit each) and compared the time it took to symbolically execute three different small programs:

1. A single Z3 bit vector array \([\text{Z3 bit vector}(8)]\). This is the most general representation based on the theory of arrays.
2. An allocation site of \(n\) bytes, create a Z3 bit vector of length \(8n\), with the entire memory modeled as a \(\text{std::map } [\text{uint} \rightarrow \text{Z3 bit vector}(8n)]\).
3. A single \(\text{std::map } [\text{uint} ightarrow \text{Z3 bit vector}(8)]\).
4. A Z3 bit vector array for each allocation site, with the entire memory modeled as a single \(\text{std::map } [\text{uint} ightarrow \text{Z3 bit vector array}]\).
5. For an allocation site of \(n\) bytes, create a \(\text{std::vector}\) of size \(n\), with each entry being an 8-bit Z3 bit vector to model a byte, and the entire memory is modeled as a single \(\text{std::map } [\text{uint} ightarrow \text{std::vector} \text{of Z3 bit vector}(8)]\).

The results are of the experiment are shown in Fig. 11.

The results show a huge difference between parallel and single-threaded solving. We believe that one possible reason for the substantial slowdown in the single-threaded case is because of cache misses when the input problem size becomes large. We have also noticed that the solver frequently suffers from memory thrashing in the single-threaded case (on a machine with 24GB of physical RAM), which further contributes to the slowdown. While one might argue that this is a relatively obvious way to speed up solving, we have compared our results with different solver implementations (Z3, yices, stp), and none of them seem to have this feature in place, possibly because constraint solvers are traditionally targeted to solving instances where most variables are related, but not instances with a large number of independent components.

Given that the time needed to do constraint splitting is relatively small as compared to the replay time (as shown in Fig. 10), it appears worthwhile to use parallel solving for replay.

5. RELATED WORK

A number of bug replay tools based on symbolic execution have been proposed recently. However, to our knowledge, no tools support partial symbolic replay for long running programs, which fundamentally distinguishes our approach. In [19], the authors proposed to record input traces during execution, and perform symbolic execution to generate bug cases for the developer. However, they used a trace logger with high overhead [17], and it is not clear if their approach is scalable to long-running programs. ESD [40] uses a path searching approach similar to model checking to reproduce bugs. It has no runtime overhead, but requires a coredump, makes no guarantee regarding how long it would take to regenerate the bug, and is tricky to use for replaying non-crash or hang bugs. ODR [13] targets multicore bugs and reproduces bugs iteratively with significant slowdowns.

Replaying executions deterministically from data logs has been a topic in systems research for many years, with the emphasis on using different mechanisms to reduce the runtime overhead and log sizes \([30, 33, 22, 17, 25]\) and recording at the operating systems level rather than application level \([27]\). Recent tools such as R2 [24] and iTarget [47] allow users to decide what data to be logged in order to reduce recording overhead, but at the expense of not being able to reproduce all executions. These tools generally have higher runtime overheads for data-intensive programs than bbr.

At the other end are techniques that automatically find bugs without any inputs. These range from static analysis tools \([16, 24, 29]\) to dynamic tools such as model checkers \([39, 38]\). Advances in SMT solvers and symbolic execution have enabled new test generation tools such as concolic testing \([32, 34]\) and other test generators based on symbolic ex-

<table>
<thead>
<tr>
<th># reqs</th>
<th># const.</th>
<th># vars</th>
<th># groups</th>
<th>single</th>
<th>split</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>8547</td>
<td>750</td>
<td>698</td>
<td>8s</td>
<td>1s</td>
</tr>
<tr>
<td>10</td>
<td>20383</td>
<td>923</td>
<td>823</td>
<td>26s</td>
<td>5s</td>
</tr>
<tr>
<td>50</td>
<td>60384</td>
<td>530</td>
<td>2314</td>
<td>32m</td>
<td>6m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impl.</th>
<th>wc</th>
<th>db connect</th>
<th>db query</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13m</td>
<td>52m</td>
<td>&gt;1hr</td>
</tr>
<tr>
<td>2</td>
<td>&gt;1hr</td>
<td>crashed</td>
<td>crashed</td>
</tr>
<tr>
<td>3</td>
<td>8m</td>
<td>15m</td>
<td>&gt;1hr</td>
</tr>
<tr>
<td>4</td>
<td>13m</td>
<td>35m</td>
<td>&gt;1hr</td>
</tr>
<tr>
<td>5</td>
<td>41s</td>
<td>1.3m</td>
<td>17m</td>
</tr>
<tr>
<td>6</td>
<td>10s</td>
<td>42s</td>
<td>2m</td>
</tr>
</tbody>
</table>

Figure 12: Memory modeling experiment results

6. We built our own data structure to represent a bit vector and implemented a number of peephole optimizations. A single \(\text{std::map } [\text{custom bit vector}(8) \rightarrow \text{custom bit vector}(8)]\) is then used to model memory. This is the implementation we used for the operations described in Section 3.2.

Fig. 12 reports different memory model implementations and their replay times. “crashed” means the experiment exhausted the address space on a 32-bit machine and crashed. As the experiment shows, using the Z3 theory of arrays incurs a substantial replay overhead in real programs, since each read / write to the array potentially creates a new array data structure. Using Z3 bit vectors still incurs some overhead in the solver, possibly due to housekeeping routines such as structural hashing. Note that the programs above were replayed from the entry point and no memory aliases were involved. We anticipate that the performance of the first 5 implementations to perform much worse in partial replay with memory aliases, and thus built our own representation of expressions at the end.
execution [23] [18]. These tools focus on finding all sorts of bugs, rather than reproducing a specific bug in hand.

Our memory model is inspired by the work done in test generation for languages that include pointer operations. In [35], the authors proposed a memory model that maintains heaps for different types of objects and introduces constraints to enforce the disjointness among the different object heaps. bbr imposes similar assumptions on object types and their alias properties. In [20], the authors proposed a region-based approach, with each address represented by a memory location object similar to that in bbr, and each location can point to different concrete addresses depending on alias resolution. In [39], a hybrid memory model was proposed with a concrete store and a symbolic store implemented using theory of arrays, which led to our initial memory model implementation. There is similar work in languages without explicit pointer constructs such as [29].

6. CONCLUSIONS

We presented bbr, a branch-deterministic replayer that performs low-overhead replay by logging only a small amount of data at runtime. We also proposed the notion of partial replay, which allows users to replay long running data-intensive programs with bounded log sizes. To make our approach scale, we introduced several new techniques, including a new memory model for handling aliased addresses, and a partitioning approach for parallel solving. We showed that these techniques allow bbr to efficiently replay a number of data-intensive programs, and can reproduce real bugs in long-running programs, including sqlite and several web servers.

7. ACKNOWLEDGEMENTS

We thank the anonymous reviewers for their valuable feedback. We also thank Lidong Zhou, Vijay Ganesh, and Nikolaj Bjørner for their helpful discussions.

References