A modified version of Robert G. Brown's "dieharder" tests for random number generators.

View license

55 stars 18 forks 6 watching Branches Activity
Tags

Public repository

1 Branch 0 Tags Go to file t Go to file Add file Code

seehuhn Merge pull request #1 from r4start/r4start--fix-linux-build

4063977 · 9 years ago

dieharder	build fixes for MacOSX	12 years ago
include	Fix compilation error "unknown ty...	9 years ago
libdieharder	build fixes for MacOSX	12 years ago
manual	build fixes for MacOSX	12 years ago
.gitignore	clean up the build system and the...	12 years ago
AUTHORS	upstream version 3.31.1	12 years ago
COPYING	upstream version 3.31.1	12 years ago
ChangeLog	upstream version 3.31.1	12 years ago
Copyright	upstream version 3.31.1	12 years ago
INSTALL	upstream version 3.31.1	12 years ago
Makefile.am	build fixes for MacOSX	12 years ago
NEWS	upstream version 3.31.1	12 years ago
NOTES	upstream version 3.31.1	12 years ago
README	clean up the build system and the...	12 years ago
autogen.sh	clean up the build system and the...	12 years ago
config.guess	upstream version 3.31.1	12 years ago
config.sub	upstream version 3.31.1	12 years ago
configure.ac	clean up the build system and the...	12 years ago
	upstream version 3.31.1	12 years ago

depcomp		
dieharder-config.in	upstream version 3.31.1	12 years ago
dieharder.abs	upstream version 3.31.1	12 years ago
dieharder.html.in	upstream version 3.31.1	12 years ago
dieharder.php	upstream version 3.31.1	12 years ago
dieharder.spec.in	upstream version 3.31.1	12 years ago
dieharder_version.h.in	upstream version 3.31.1	12 years ago
install-sh	upstream version 3.31.1	12 years ago
missing	upstream version 3.31.1	12 years ago
mkinstalldirs	upstream version 3.31.1	12 years ago

```
This is a modified version of the diehard random number generator
testing suite.  See http://www.phy.duke.edu/~rgb/General/dieharder.php
for Robert Brown's original version.

========================================================================

            Building Dieharder
========================================================================

You MUST run ./autogen.sh FIRST.  Then ./configure, make and so on
should work.  Sorry, if I distribute it any other way some aspect of the
Gnu Build Tools breaks for some system.  See INSTALL for more details.

========================================================================

Author Contact Information:

   Robert G. Brown
   Duke University Dept. of Physics, Box 90305
   Durham, N.C. 27708-0305
   Phone: 1-919-660-2567
   Fax: 919-660-2525
   Email: rgb@phy.duke.edu
   URL: http://www.phy.duke.edu/~rgb

========================================================================

                Versioning

Versioning in dieharder has a very specific meaning.  The major number
is bumped when a major project milestone is reached OR when a major
fundamental redesign takes place (something that happens roughly 3-5
times over the lifetime of any given project).  The first minor is the
number of tests built into the current snapshot.  The second minor is
bumped when e.g. a major change occurs within a release -- a bug is
fixed, a new feature (but not a new test) is added.  Release is used to
track micro/testing releases in the development cycle.  Basically,
proposed bugfixes that will eventually become bumps in the second minor
number.


In this way one can always see if dieharder is likely to have major new
```

features or bugfixes in it relative to your current version.

Notes About the Tests in Dieharder

Dieharder is original code written by and Copyright Robert G. Brown (with different code modules written over the period 2003-present). The tests included (or expected to be included in the future) in dieharder, are, however, derived from descriptions from several places.

* Diehard, a famous suite of random number tests written over many years by George Marsaglia. The original Diehard sources (written in Fortran) are (of course) Copyright George Marsaglia according to the Berne convention, where authors retain copyright with or without a notice in any original work. The original Diehard code written by Marsaglia did not include a copyright notice or an explicit license in or with the sources that have been made publically available on the web for many years. When contacted, Dr. Marsaglia has indicated his wish to restrict commercial usage of his code and permit only academic/research related use. For this reason the the algorithms are fully re-implemented, in original code, in dieharder to keep authorship and GPL licensing issues clear. However, all diehard-equivalent tests are clearly labelled as such and academically attributed to Dr. Marsaglia.

* The National Institute of Standards and Technology (NIST) Statistical Test Suite (STS) as described in publication SP800-22b. Although this test suite was developed with government support and is explicitly in the public domain, and is available in C source. There is some overlap between STS and Diehard -- for example, both have binary matrix rank tests -- but the STS focusses primarily on bitlevel randomness and the suitability of a random number generator for use in cryptographic applications. The tests described in SP800-22b that are implemented in dieharder are completely rewritten in original C by Robert G. Brown to keep copyright and GPL issues clear. All STS-derived tests are clearly labelled as such and are academically attributed to the various authors of the suite (Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo).

* Original tests or timing operations inserted by Robert G. Brown. Almost any distribution that can be computed on the basis of a source of random numbers with a derived statistic with known or reliably measurable statistical properties can serve as a test of random numbers using the general approach implemented in Diehard, the STS, Dieharder, and elsewhere.

* Tests described in Knuth's The Art of Computer Programming.

* User-contributed tests.

* Tests described elsewhere in the literature.

In all cases some effort has been made to correctly attribute the originator of a test algorithm, and if there are any errors in this regard they will be happily corrected once they are brought to the attention of the author.

===

To Build Dieharder

See the file INSTALL that should have come with the tarball to get fairly explicit building instructions. You may have to experiment a bit to figure out the dynamic linking thing mentioned there and below in

README License

Development and Experimentation

Dieharder is an open source project for a reason -- it simply is not possible to trust a test suite of this sort without access to the source because even a subtle error in the sources or data used to perform a test will cause the test to return incorrect answers, conceivably to the detriment of all concerned. With the source readily available, any user is free to examine or modify the source for any test and determine whether or not the test is working and participate in the critical process whereby academia arrives at a consensus truth.

Also, many individuals may wish to use the general dieharder library to test their own (software) rngs. This may well involve adding tests or modifying individual tests already there, or dieharder defaults. dieharder is built using the familiar, if somewhat evil, Gnu Build Tools. Unpack tarball, run autogen.sh, ./configure, make. If you wish to install, be sure to set the prefix. Be aware that this program builds a DYNAMICALLY LINKED version of the program. If you want a statically linked version or to be able to work on it in the build directory either add the libdieharder directory to your LOAD_LIBRARY_PATH or hack the Makefile.am to build and use a static library (the commands are there, commented out).

RPM

Dieharder is developed on RPM-based systems (FCX) and one should be able to build an RPM by using the make target: "make rpm" (after setting up a private RPM build tree). No root privileges are needed to build the rpms in this way.

Debian / Ubuntu

Dieharder has been in Debian since February 2007. Therefore, on most current Debian or Ubuntu systems a simple

```
   sudo apt-get install dieharder
```

installs the command-line (which itself also install the shared library package it depends upon). In order develop against the Dieharder API, run

```
   sudo apt-get install libdieharder-dev
```

===

Licensing and Revision Control

Dieharder is (as noted) Copyright Robert G. Brown, 2003-2006. It has been kept under revision control (first CVS, more recently Subversion) since the inception of the process in 2003 and all incremental changes to the code as it was developed are carefully documented.

Dieharder was deliberately developed to be a GPL project, since alternative random number test suites were either incomplete with regard to the span of test possibilities of interest to the author, restricted or unclear about their licensing restrictions, or both. In addition, by integrating from the beginning with the Gnu Scientific Library (which is a full GPL project with the viral version of the license) it becomes itself a GPL project in any event.

It is strongly suggested that prospective users of this test read the terms of the license included with this source distribution in the file COPYING. In summary, permission is granted to freely use and modify the sources and distribute the result or any binary objects derived therefrom as long as the terms of the GPL are abided by. These terms require the preservation of all copyright and license information in the sources and that the source of any and all revisions to the original dieharder code be made available upon request to any receivers of a dieharder binary, among other things.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

```
    If any user of the dieharder program should revise the program in a way
    that is likely to be of use to others, they are encouraged to at least
    offer to contribute the revision back to the project (subject to the
    "editorial" approval of the primary author).  Contact Robert G. Brown to
    arrange for such a contribution.

    ========================================================================
```

Releases

No releases published

Packages

No packages published

Contributors 2

seehuhn Jochen Voss

r4start r4start

Languages

● **C** 70.0% ● **TeX** 22.6% ● **Roff** 3.2% ● **Shell** 2.4% ● **Makefile** 1.0% ● **M4** 0.4% ● **Other** 0.4%