Pre-Qualification of a Mathematical Library for Flight Software

TEC-ED & TEC-SW Final Presentation Day

May 2018

Andoni Arregi (GTD GmbH)

Contents Overview

- Why it is relevant to qualify a math library for flight software
- What we did to qualify it on representative targets
- What the user gets in the form of a qualification kit

Motivation

- Why do we need this activity?
  - It has not been done before. There is no math library with full life-cycle documentation and complete test-suite for qualification available.
  - We do not get the same results when computing an algorithm on a PC or on an embedded target.
  - We do not know what the contribution to numerical errors of elementary mathematical functions is.
  - We do not know what the execution time behavior over the floating point domain of such functions is.

Activity & Objectives

- Development of a basic mathematical library containing elementary mathematical functions, ready for qualification

MLFS

Mathematical Library for Flight Software

- Development of a test suite to provide qualification evidence
- ESA GSTP Activity (4000117691/16/NL/FE)

Requirements to the Library

- Provide elementary mathematical functions needed for AOCS/GNC algorithms
- Be ISO C99 and POSIX compliant
- Yield results reproducible on x86-64 and SPARC V8 platforms
- Provide a good and known accuracy
- Guarantee a good WCET behavior and reasonable size

Requirements to the Test Suite

- Provide a comprehensive test suite for validating elementary mathematical functions
- Provide execution capability on target (SPARC V8) and host (x86-64) systems
- Provide detailed reports on results to support the qualification of the library
- Provide means to assess the accuracy and timing behavior of the library

Starting Point for the Library

- Development from scratch vs. re-engineering
- Alternatives for re-engineering:
  - Glibc libm: uses IBM Accurate Mathematical library. High accuracy but complex implementation.
  - Newlib libm: widely used for embedded systems.
  - FreeBSD libm: focus on accuracy and optimizations for x86 systems.
  - Correct rounding libraries (CRLibm, libmcr, &c.): no acceptable WCET (x10…x1000)

Starting Point for the Library

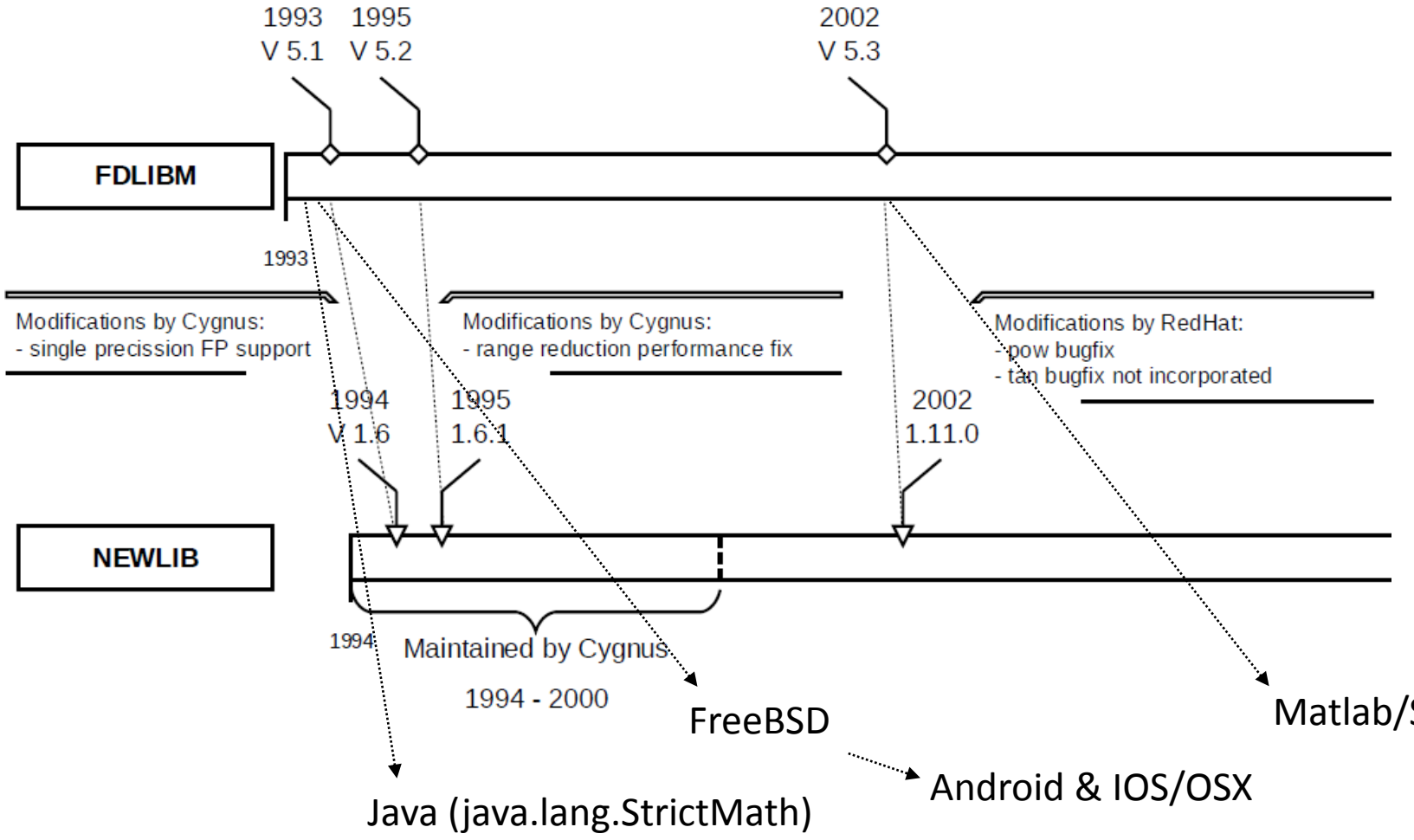
- Newlib 2.4.0 libm (reduced to the functions included in MLFS)
  - LoC: 3221 (total lines: 10204)
  - Functions: 82 (including float and double versions)
  - Cyclomatic complexity: 35 functions above 10 (max 68)
- Reuse approach:
  - Strong heritage -> modifications to be done with care
  - Objective: best possible offspring of FDLIBM in terms of accuracy, portability and performance (average and WCET)

History of the Newlib Libm

- It has its origins in developments done in 1985 at University of California in Berkeley (by people close to W. Kahan, author of IEEE-754 floating-point standard)
- These developments ended up in the FreeBSD libm and in FDLIBM (freely distributed by Sun Microsystems in 1993)
- Since then it is integrated in many products and SW systems

It has a very strong heritage

History of the Newlib Libm



MLFS Features

- 32 bit (float) and 64 bit (double) floating-point versions of the procedures
- Included procedures:
  - Classification macros: `fpclassify, isfinite, isinf, isnan, isnormal, signbit`
  - Trigonometric functions: `acos, asin, atan, atan2, cos, sin, tan`
  - Exponential and logarithmic functions: `exp, log, log10, modf`
  - Power and absolute value functions: `fabs, hypot, pow, sqrt`
  - Nearest integer functions: `ceil, floor, round, trunc`
  - Remainder functions: `fmod`
  - Manipulation functions: `copysign`
  - Maximum, minimum, and positive difference functions: `fmax, fmin`
  - Conversion functions: `deg2rad, rem2pi`

MLFS Features

- Size: ~40 kB on SPARC 8 and on x86-64
- Maximal accuracy error: ~1.5 ULP (atan2f)
- Reproducible results on SPARC V8 and x86-64

Development of MLFS

- Improvements:
  - Correction of severe accuracy bug in trigonometric functions (sinf, cosf, tanf)
  - Other accuracy improvements from FreeBSD (expf, hypotf, log10/f, pow/f, atan2/f, asin, atan, cos/f, sin/f, tan/f)
  - Introduction of Denormals Are Zero (DAZ) modus for FPUs not handling Subnormal numbers such as the Gaisler GRFPU
  - Robustness regarding null pointer parameters
  - Use of volatile variables to enforce correct exception generation
  - Fixing POSIX behaviors in several functions (e.g., modf, pow)
  - Fixing POSIX noncompliant behaviors regarding NaN handling

Development of MLFS

- Improvements:
  - Addition of choice to use HW sqrt implementation
  - Fixing/justifying MISRA C:2012 guideline violations (>2700)
  - Improving portability between compilers
  - Correcting comments
  - Fixing issues with typing, comparisons, unused variables, garbage initializations, &c.

Development of MLFS

- Accuracy improvements

Float functions (1e9 values tested)		
Function name	**Newlib 2.4.0**	**MLFS**
acos	0.889	0.889
asin	0.901	0.901
atan2	**1.480**	**1.480**
atan	0.844	0.844
cos	**6739672.986**	0.788
deg2rad		0.630
exp	0.892	0.892
hypot	**1.195**	**1.150**
log10	**2.032**	0.818
log	0.869	0.869
pow	**134.518**	**1.000**
rem2pi		**1.000**
sin	**8476449.076**	0.787
sqrt	0.500	0.500
tan	**13018076.800**	0.965

Double functions (4e9 values tested)		
Function name	**Newlib 2.4.0**	**MLFS**
acos	0.878	0.878
asin	0.848	0.848
atan2	**1.513**	**1.513**
atan	0.847	0.847
cos	0.856	0.792
deg2rad		0.652
exp	0.885	0.885
hypot	**1.082**	**1.082**
log10	**1.880**	0.682
log	0.853	0.853
pow	**1.000**	0.886
rem2pi		**1.000**
sin	0.864	0.798
sqrt	0.500	0.500
tan	0.928	0.928

Testing with the BLTS

- Unit tests: 4042 (for 92 functions)
  - 100% statement and branch coverage on target
  - 100% MC/DC coverage on source code
- Validation tests: (for 50 functions)
  - 396 for requirement coverage, 617 for accuracy
  - 70 M values tested (limited by memory transfer from target to host)
  - 128 bit reference values: MPFR multiple precision library

BLTS Reporting

- The test report:

Workspace Summary Report: 'E1356-GTD-SVS-02'

BLTS version: v1.2
BLTS md5: 18270eacf6f8fab5db064f445b2e6acff6 /home/engineer/blts_install/bin/blts_app

Target information

Name	GR-CPCI-AT697-EDISOFT
Toolchain	/opt/rtems-4.8
CrossCompile	sparc-rtems4.8-
MakeOptions	PLATFORM=EDISOFT CPU=leon2 clean
CFLAGS	N/A
Compiler version	gcc version 4.2.1
Compiler MD5	e7cf4f259245e717acac9fdbdb40f3b9 /opt/rtems-4.8/bin/sparc-rtems4.8-gcc
Processor	04:002 ESA LEON2 SPARC V8 Processor (ver 0x0)
FPU Status	ON

External libraries

Name	mathlib
Version	1.2 c07acbf539f6880d8c1255e7f85138b89f33387b
CFLAGS	-I/home/engineer/E1356-GTD-BL-01/include -I/home/engineer/E1356-GTD-BL-01/libm/common -I/home/engineer/E1356-GTD-BL-01/libm/mlfs
LDFLAGS	-L/home/engineer/E1356-GTD-BL-01/build-sparc_v8/bin -lmlfs
lib MD5	a36438a6a2b68f2d25deda3a26dc001c /home/engineer/E1356-GTD-BL-01/build-sparc_v8/bin/libmlfs.a
Coverage data	N/A
MPFR Version	3.1.5

Reporting configuration

ULP Cutoff	0.5
Relative error float cutoff	5.961e-8
Relative error double cutoff	1.111e-16
Denormals are zero	NO

Single-value Tests

Session	Function	Total Run / Defined	Passed	Failed	Run date
acosf_validation-normal	acosf	6 / 6	6	0	2018-04-20T15:43:40Z
acos_validation-normal	acos	6 / 6	6	0	2018-04-20T16:58:28Z
asinf_validation-normal	asinf	7 / 7	7	0	2018-04-20T17:45:04Z
asin_validation-normal	asin	7 / 7	7	0	2018-04-20T18:56:45Z
atan2f_validation-normal	atan2f	25 / 25	25	0	2018-04-20T21:09:34Z
atan2_validation-normal	atan2	25 / 25	25	0	2018-04-21T00:53:44Z
atanf_validation-normal	atanf	5 / 5	5	0	2018-04-21T01:21:52Z
atan_validation-normal	atan	5 / 5	5	0	2018-04-21T01:59:08Z
ceilf_validation-normal	ceilf	5 / 5	5	0	2018-04-21T02:06:45Z
ceil_validation-normal	ceil	5 / 5	5	0	2018-04-21T02:11:24Z
copysignf_validation-normal	copysignf	1 / 1	1	0	2018-04-21T02:14:18Z
copysign_validation-normal	copysign	1 / 1	1	0	2018-04-21T02:17:36Z

BLTS Reporting

- The test report:

Range Tests

Session	Function	Total Run / Defined	ULP difference			Max Absolute error	Relative error			Run date
			<=cutoff	>cutoff	Max		<=cutoff	>cutoff	Max	
acosf_validation-normal	acosf	1986778 / 1986778	1850630	136148	8.7898e-01	2.0956e-07	1946140	40638	9.9081e-08	2018-04-20T15:43:40Z
acos_validation-normal	acos	1986778 / 1986778	1853696	133082	8.7602e-01	3.8903e-16	1986778	0	1.8476e-16	2018-04-20T16:58:28Z
asinf_validation-normal	asinf	1992738 / 1992738	1931332	61406	8.9112e-01	8.9456e-08	1975320	17418	9.9739e-08	2018-04-20T17:45:04Z
asin_validation-normal	asin	1920418 / 1920418	1860220	60198	8.3693e-01	1.6645e-16	1920418	0	1.7413e-16	2018-04-20T18:56:45Z
atan2f_validation-normal	atan2f	5080709 / 5080709	4413393	667316	1.4118e+00	2.5076e-07	4857197	223512	3.2421e-01	2018-04-20T21:09:34Z
atan2_validation-normal	atan2	4656933 / 4656933	3947329	709604	1.3988e+00	4.9106e-16	4656933	0	2.4405e-16	2018-04-21T00:53:44Z
atanf_validation-normal	atanf	993539 / 993539	992191	1348	7.6242e-01	8.7991e-08	993389	150	7.4565e-08	2018-04-21T01:21:52Z
atan_validation-normal	atan	1008423 / 1008423	1008195	228	7.2154e-01	1.5056e-16	1008423	0	1.3298e-16	2018-04-21T01:59:08Z
ceilf_validation-normal	ceilf	108627 / 108627	108627	0	0.0000e+00	0.0000e+00	108627	0	0.0000e+00	2018-04-21T02:06:45Z
ceil_validation-normal	ceil	93267 / 93267	93267	0	0.0000e+00	0.0000e+00	93267	0	0.0000e+00	2018-04-21T02:11:24Z
copysignf_validation-normal	copysignf	53377 / 53377	53377	0	0.0000e+00	0.0000e+00	53377	0	0.0000e+00	2018-04-21T02:14:18Z
copysign_validation-normal	copysign	53377 / 53377	53377	0	0.0000e+00	0.0000e+00	53377	0	0.0000e+00	2018-04-21T02:17:36Z
cosf_validation-normal	cosf	2659353 / 2659353	2630059	29294	7.5462e-01	4.4979e-08	2659033	320	6.5017e-08	2018-04-21T03:03:50Z
cos_validation-normal	cos	2659353 / 2659353	2626933	32420	7.5342e-01	8.3647e-17	2659353	0	1.2291e-16	2018-04-21T04:41:55Z
deg2radf_validation-normal	deg2radf	1426582 / 1426582	1308424	118158	6.2983e-01	3.5751e+29	1292724	133858	3.3246e-01	2018-04-21T05:20:40Z
deg2rad_validation-normal	deg2rad	1426582 / 1426582	1277444	149138	6.5108e-01	3.4678e+290	1426582	0	5.6045e-14	2018-04-21T06:13:08Z
expf_validation-normal	expf	1488582 / 1488582	1437418	51164	8.6283e-01	1.5007e+31	1448264	40318	3.3316e-01	2018-04-21T06:46:38Z
exp_validation-normal	exp	1488582 / 1488582	1439941	48641	8.6478e-01	1.3226e+292	1488582	0	2.1296e-14	2018-04-21T07:41:50Z
fabsf_validation-normal	fabsf	91219 / 91219	91219	0	0.0000e+00	0.0000e+00	91219	0	0.0000e+00	2018-04-21T07:51:54Z
fabs_validation-normal	fabs	91219 / 91219	91219	0	0.0000e+00	0.0000e+00	91219	0	0.0000e+00	2018-04-21T07:56:23Z
floorf_validation-normal	floorf	93267 / 93267	93267	0	0.0000e+00	0.0000e+00	93267	0	0.0000e+00	2018-04-21T07:59:28Z
floor_validation-normal	floor	93267 / 93267	93267	0	0.0000e+00	0.0000e+00	93267	0	0.0000e+00	2018-04-21T08:04:07Z
fmaxf_validation-normal	fmaxf	56125 / 56125	56125	0	0.0000e+00	0.0000e+00	56125	0	0.0000e+00	2018-04-21T08:07:00Z
fmax_validation-normal	fmax	56125 / 56125	56125	0	0.0000e+00	0.0000e+00	56125	0	0.0000e+00	2018-04-21T08:10:22Z
fminf_validation-normal	fminf	56125 / 56125	56125	0	0.0000e+00	0.0000e+00	56125	0	0.0000e+00	2018-04-21T08:12:30Z
fmin_validation-normal	fmin	56125 / 56125	56125	0	0.0000e+00	0.0000e+00	56125	0	0.0000e+00	2018-04-21T08:15:51Z
fmodf_validation-normal	fmodf	56125 / 56125	56125	0	0.0000e+00	0.0000e+00	56125	0	0.0000e+00	2018-04-21T08:18:03Z
fmod_validation-normal	fmod	56125 / 56125	56125	0	0.0000e+00	0.0000e+00	56125	0	0.0000e+00	2018-04-21T08:21:30Z
hypotf_validation-normal	hypotf	6108133 / 6108133	5792333	315800	1.0141e+00	inf	6014277	93856	2.9289e-01	2018-04-21T10:48:20Z
hypot_validation-normal	hypot	7275493 / 7275493	7129257	146236	9.9423e-01	3.4712e+291	7275493	0	1.2754e-14	2018-04-21T16:30:20Z
log10f_validation-normal	log10f	996483 / 996483	991305	5178	8.0339e-01	1.9156e-06	996299	184	6.6972e-08	2018-04-21T17:01:43Z
log10_validation-normal	log10	996483 / 996483	996406	77	5.9571e-01	2.8423e-14	996483	0	1.1849e-16	2018-04-21T17:39:27Z
logf_validation-normal	logf	997643 / 997643	991991	5652	7.9210e-01	3.8361e-06	997387	256	8.1930e-08	2018-04-21T18:03:09Z
log_validation-normal	log	993483 / 993483	992399	1084	7.5410e-01	5.6878e-14	993483	0	1.3953e-16	2018-04-21T18:40:37Z
modff_validation-normal	modff	942963 / 942963	942963	0	0.0000e+00	0.0000e+00	942963	0	0.0000e+00	2018-04-21T19:10:05Z
modf_validation-normal	modf	942963 / 942963	942963	0	0.0000e+00	0.0000e+00	942963	0	0.0000e+00	2018-04-21T20:00:46Z
powf_validation-normal	powf	5406254 / 5406254	5319416	86838	9.9986e-01	1.4607e+31	5342412	63842	1.0000e+00	2018-04-21T22:18:36Z

BLTS Reporting

- The coverage report:

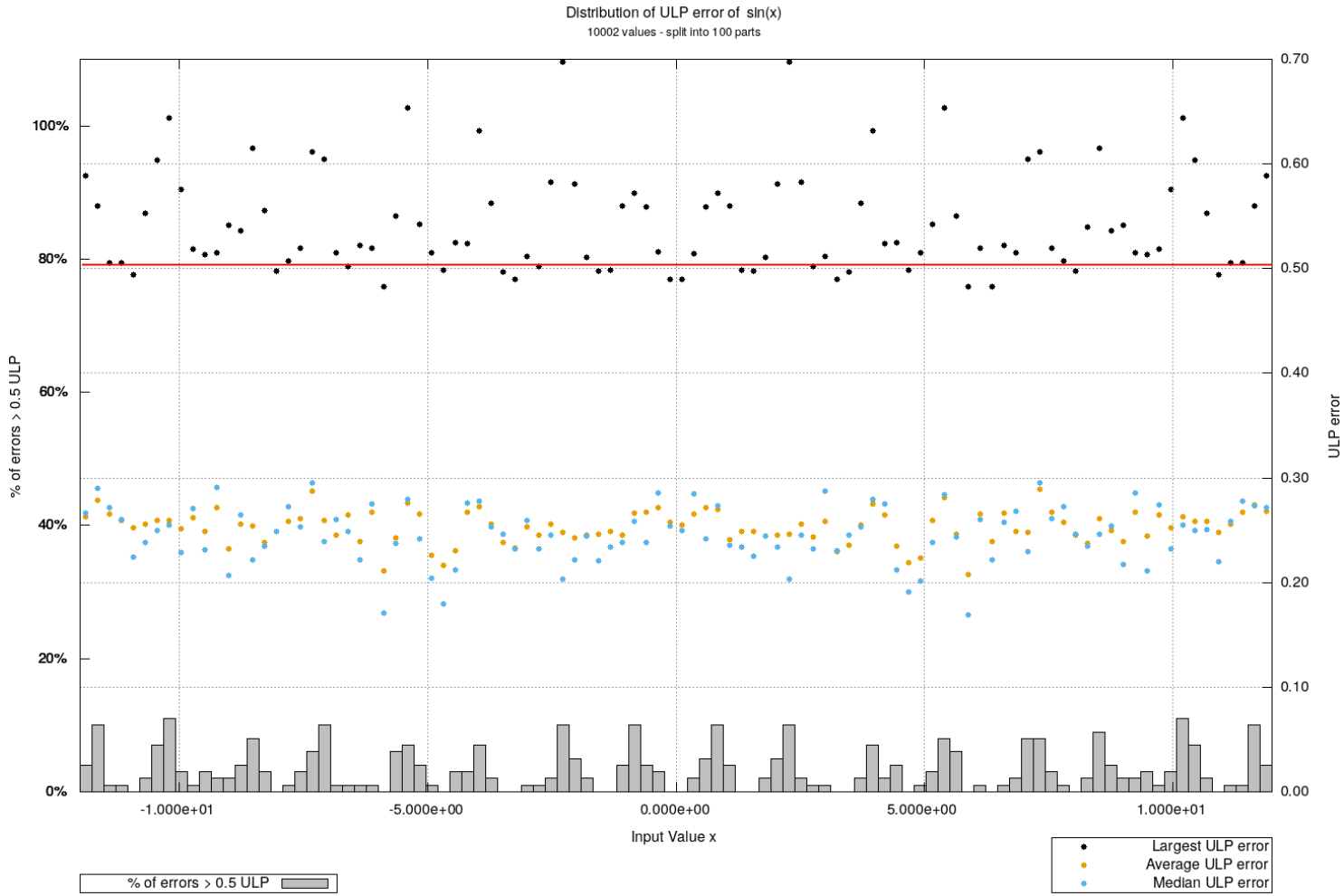
LCOV - code coverage report

		Hit	Total	Coverage
Current view: top level - common	Lines:	245	245	100.0 %
Test: unit_host_cov.info	Functions:	20	20	100.0 %
Date: 2017-09-06 16:54:34	Branches:	174	174	100.0 %

Filename	Line Coverage		Functions		Branches	
s_copysign.c	100.0 %	5 / 5	100.0 %	1 / 1	-	0 / 0
s_fmax.c	100.0 %	6 / 6	100.0 %	1 / 1	100.0 %	6 / 6
s_fmin.c	100.0 %	6 / 6	100.0 %	1 / 1	100.0 %	6 / 6
s_fpclassify.c	100.0 %	15 / 15	100.0 %	1 / 1	100.0 %	30 / 30
s_modf.c	100.0 %	32 / 32	100.0 %	1 / 1	100.0 %	14 / 14
s_nan.c	100.0 %	3 / 3	100.0 %	1 / 1	-	0 / 0
s_round.c	100.0 %	29 / 29	100.0 %	1 / 1	100.0 %	18 / 18
s_scalbn.c	100.0 %	21 / 21	100.0 %	1 / 1	100.0 %	16 / 16
s_signbit.c	100.0 %	6 / 6	100.0 %	2 / 2	-	0 / 0
s_trunc.c	100.0 %	13 / 13	100.0 %	1 / 1	100.0 %	8 / 8
sf_copysign.c	100.0 %	5 / 5	100.0 %	1 / 1	-	0 / 0
sf_fmax.c	100.0 %	6 / 6	100.0 %	1 / 1	100.0 %	6 / 6
sf_fmin.c	100.0 %	6 / 6	100.0 %	1 / 1	100.0 %	6 / 6
sf_fpclassify.c	100.0 %	13 / 13	100.0 %	1 / 1	100.0 %	22 / 22
sf_modf.c	100.0 %	23 / 23	100.0 %	1 / 1	100.0 %	10 / 10
sf_nan.c	100.0 %	3 / 3	100.0 %	1 / 1	-	0 / 0
sf_round.c	100.0 %	18 / 18	100.0 %	1 / 1	100.0 %	10 / 10

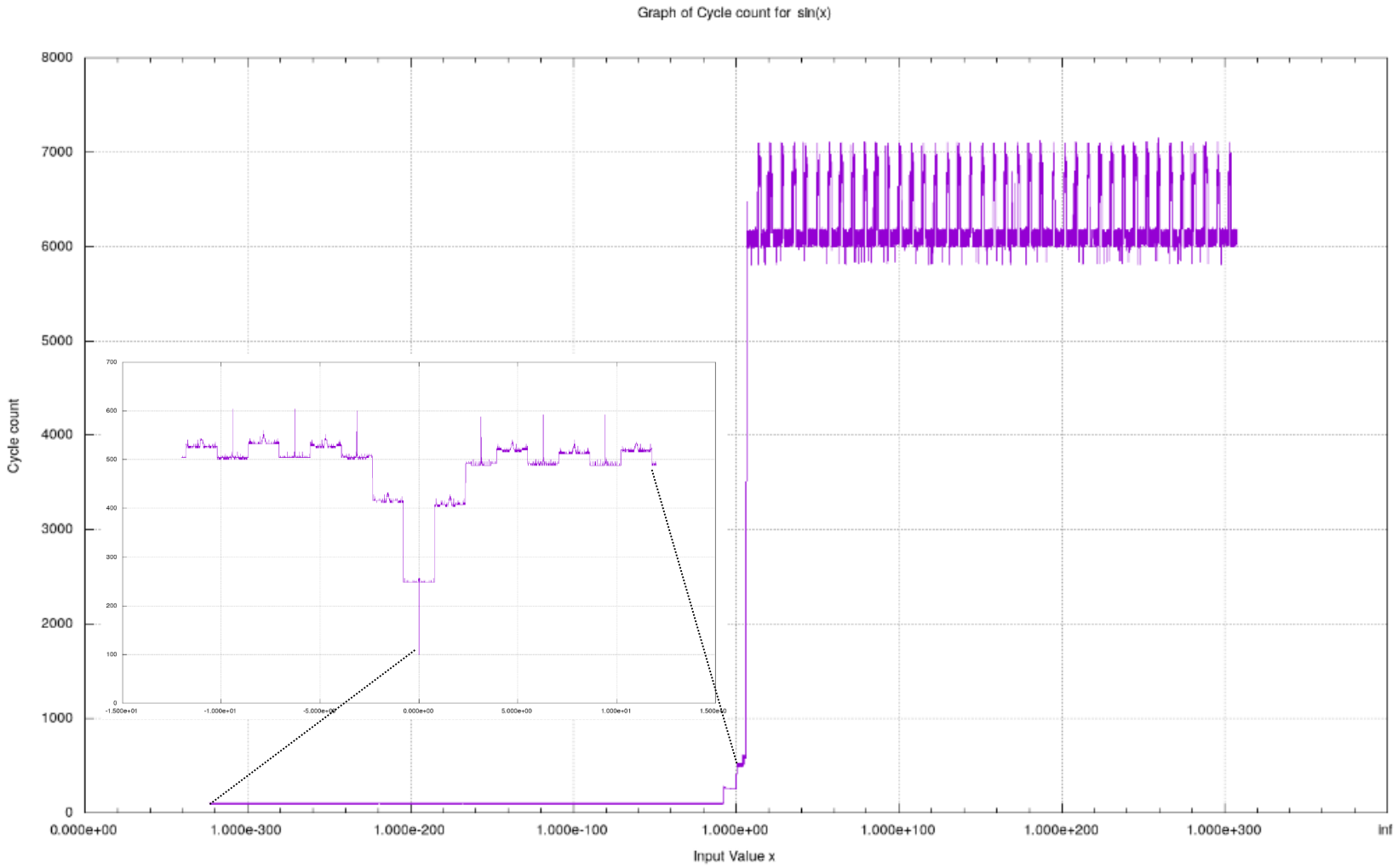
BLTS Reporting

- The accuracy report:
  - sin(x) 64 bit double function
  - x in [-12,12]
  - Errors in ULP
    - <0.5 ULP for exact results
    - <1 ULP only last bit incorrect



BLTS Reporting

- The timing report:
  - sin(x) 64 bit double function
  - Cycle count on LEON2
  - Different execution time in different subdomains



Additional Verification & Testing by ESA

- Basic Library Extensive Testing Tool (BLET):
  - 16000 M values tested, mainly on x86-64
- Static analysis of the source code:
  - Clang Static Analyzer
  - Carnegie Mellon's Bounded Model Checker (CBMC)
  - Mathworks Polyspace Bug Finder and Code Prover
  - RougeWave Klockwork

MLFS Qualification Kit

- Basic mathematical Library (BL)
  - Source code
  - ECSS E-ST-40 and Q-ST-80 compliant documentation for category B software (limitations defined in SRelD)
- Test Suite (BLTS)
  - Source code and corresponding documentation
  - Unit and validation test cases
- Validation evidences on two representative targets:
  - LEON2 (Atmel AT697E with Meiko FPU)
  - LEON4 (N2X with GRFPU)

MLFS Qualification Guideline

- Configure in the BLTS the:
  - Compilation toolchain (including compilation flags and OS information)
  - Target specific parameters
- Run the BLTS with the provided unit and validation tests
- Verify the resulting reports for:
  - Accuracy
  - Timing
  - Coverage
- Provide validation evidence attaching the reports to an SValR
- Perform a HW/SW Interaction Analisys (HSIA) for the specific target
- Notify found nonconformances to the MLFS maintenance

Contacts and Qualification Kit

- Technical Officer at ESA:
  - Andreas Jung: andreas.jung@esa.int
- Project Manager at Prime (GTD GmbH)
  - Andoni Arregi: andoni.arregi@gtd-gmbh.de

- Qualification Kit will be available on:
  - European Space Software Repository: https://essr.esa.int/