Ada 2012 Nearing Completion

Next Version of Language Standards Offers Numerous Enhancements

As part of the natural evolution of the language design, a new version of the Ada standard is nearing completion. Referred to as Ada 2012, this is an upwards compatible increment to Ada 2005. A number of new features are currently under consideration, including:

- Improved support for specifying assertions (membership predicates for subtypes, pre- and postconditions for subprograms, invariants for packages and types, global in-out annotations);
- Improved support for real-time and concurrent programming (multiprocessor Ravenscar, barriers, task/processor affiliities, task-safe queues);
- Bound sequences of the container packages appropriate in applications that cannot use dynamic storage allocation or controlled types;
- Improved support for iterating over the elements of a container or array;
- More flexible forms of expressions (if-expressions, case-expressions, quantified expressions, more general membership test);
- Improved support for controlling visibility of names (use all type, integrated packages);
- Region-based memory management via subpools of storage pools;
- "in out" and "out" mode parameters for functions;
- New uses for incomplete types (to introduce a private type, as a parameter or result type, as a generic formal parameter);

For details, please see www.open-do.org/05-summary.html.

As their design firms up, many of these features are being prototyped in the GNAT technology (for example if- and case-expressions), allowing customers to gain early experience. With this phased approach, comprehensive support for Ada 2012 is expected soon after the final language definition is approved.

Open-DO Update

Launched in early 2009, the Open-DO initiative promotes using open source software and lean / agile methodology in developing and certifying high-integrity systems. This year’s Open-DO conference took place in Paris on March 11 and focused on how to combine formal methods with agile development. Notable speakers included Whitehall (Delphi (Airbus), Peter Gardner (Silver Atama) and Paul Boc (Hornbill Systems). Videos of the conference are available at http://www.open-do.org/conference-2010. The Open-DO community web site now has more than 100 registered members, who can comment on posted articles through a blog-like interface. Several new projects have also joined the Open-DO forge, including Couverture and the Qualifying Machine. More information on the Open-DO initiative can be found on www.open-do.org, and the Open-DO forge can be accessed on www.forge.open-do.org.

CodePeer Launched

The CodePeer source code analyzer / reviewer for Ada is now available. This tool identifies constructs that are likely to lead to run-time errors such as buffer overflows, and it flags legal but suspect code indicative of logic errors. With surpassing typical static analysis tools, CodePeer also produces a detailed analysis of each subprogram, including pre- and postconditions. Potential bugs and vulnerabilities can thus be accurately diagnosed early. If the specification declared by CodePeer does not match the component’s requirements, a reviewer is alerted immediately to a likely logic error.

CodePeer can be used productively during program development and upgrade, to prevent errors from being introduced or to augment a systematic code inspection process and thus maximize the efficiency of human review. It can also be used effectively on existing codebases, to detect and remove latent bugs.

CodePeer analyzes Ada programs for a wide range of flaws including pointer misuse, buffer overflows, "false positives" (flagged constructs that are not real errors) since the user does not need to review the output for unchanged parts of the program. Moreover, CodePeer can work on partially complete programs, so units can be analyzed as required.

AdaCore was developed jointly by AdaCore and SoftCheck and may be used either as a stand-alone tool or integrated into the GNAT Pro environment. For further information: www.adacore.com/home/products/codepeer.
GNAT Pro 6.3

This major release is available on more than fifty native and cross platforms comprising hundreds of different environments (variations of Ada run-time libraries and host/target Operating System versions). Highlights include:

- CodeReps, a new add-on tool for automated code review and validation.
- C++ support as an option, for projects using C++ as well as Ada.
- Global tool improvements to the pretty printer, gnatdoc, coding standard verifier (gnatchck), stack size analyzer (gnatstack), and the C and C++ binding generators.
- Specific tool improvements:
  - Unused dispatching subprogram elimination (gnatelim)
  - More flexible project handling
  - More efficient gnatmake and gprbuild
- Compiler and debugger enhancements
- Many additional warnings
- More flexibility in enabling/disabling warnings
- Faster unbound register implementation
- Removal of redundant run-time checks
- Support for Ada 2012 conditional expressions
- Better code generation (speed and size)
- More compact debugging information
- Improved interfacing with C++

The 6.4 release also includes the latest versions of the GNAT Programming Studio (GPS 4.4) and GNATbench (2.6). GPS 4.4 is compatible with GNAT Pro versions 3.16 and up to 6.3.

SPARK Pro 9.0

The latest version of SPARK Pro, a joint offering from AdaCore and Altran Praxis, is a major release with many enhancements:

- New information-flow verification for safety and security policies, such as Bell LaPadula, based on integrity labelling of own variables.
- New SPARK 2005 language profile, including Mod, Machine_Rounding, new renamed words, and the static semantics of “overriding.”
- Detection of dead statements, branches and paths in SPARK code, complementing the Simulator and POGS.
- Cross Referencing annotations in GPS.
- Treatment of function annotation semantics like procedure post-conditions. The annotations are substituted into the caller’s VCs hypotheses, thus greatly improving the theorem prover’s effectiveness.
- A new output format for POGS designed to be both easier to read and easier to search automatically.
- Case checking, through a new Examiner switch that enforces consistent casing within code and annotations.

GPRbuild 1.4

The latest release of GPRbuild, a tool for generating systems written in a combination of programming languages, offers a number of enhancements.

- There is more precision at detecting implicit coupling between subprograms no-integer imports. Performance is greatly improved on large projects, especially when project files are used, since the number of system calls has been significantly reduced. GPRbuild also supports new configurations including Apple Snow Leopard, Win32/Lynx, LynxOS 5, and VxWorks.

Webinar Schedule

Tuesday, April 27 / SPARK Pro 9.0

The InSight webinar series continues this Spring with a presentation by Robin Mesier (Altran Praxis) on the new version of SPARK Pro, the AdaCore / Altran Praxis joint offering. The webinar discusses and demonstrates the new features of this major release and includes a question and answer session. To register, please visit www.adacore.com/home/products/gnatpro/webinars.

SPARK Pro 9.0

Case checking, through a new Examiner switch that enforces consistent casing within code and annotations.

GPRbuild 1.4

The latest release of GPRbuild, a tool for generating systems written in a combination of programming languages, offers a number of enhancements.

- There is more precision at detecting implicit coupling between subprograms no-integer imports. Performance is greatly improved on large projects, especially when project files are used, since the number of system calls has been significantly reduced. GPRbuild also supports new configurations including Apple Snow Leopard, Win32/Lynx, LynxOS 5, and VxWorks.

Webinar Schedule

Tuesday, April 27 / SPARK Pro 9.0

The InSight webinar series continues this Spring with a presentation by Robin Mesier (Altran Praxis) on the new version of SPARK Pro, the AdaCore / Altran Praxis joint offering. The webinar discusses and demonstrates the new features of this major release and includes a question and answer session. To register, please visit www.adacore.com/home/products/gnatpro/webinars.

Interview with José Ruiz

Senior Software Engineer, AdaCore EU

Tell us about your background and how you came to be involved with Ada and AdaCore. What is your current role?

…I discovered Ada as a student at the Technical University of Madrid, thanks to Professors Juan Antonio de la Puente and Alejandro Alonso. My first major Ada project involved porting the Ada core run-time system to bareboard PICs, and I was fascinated by the embedded world where you control everything that is executing on your system. Then, during my Ph.D. work, I helped implement a run-time library supporting the Ravenscar profile for space processors. That project tightened my relationship with AdaCore and subsequently led to an offer to join their Paris office. This was an excellent career opportunity, and my wife liked the prospect of living in Paris, so saying “yes” was an easy decision.

Here at AdaCore I’m working on applied research for safety-critical embedded real-time systems. Projects include adapting Ravenscar towards new functionalities and targets, and exploring qualification and certification solutions for high-integrity software. I also work on GNAT technology development, and I’ve recently been implementing some enhancements to GNATStack.

AdaCore has been providing software development solutions for high-integrity systems for many years. How do you see the marketplace evolving, and what is AdaCore doing to meet the new demands?

…I see an encouraging increase in the number of new projects focusing on safety aspects. Systems are growing in size and complexity—not only in our traditional markets like aerospace but also in others such as automotive. With the safety and economic implications of failures in these systems, I expect high-integrity methodologies to be much more widely embraced in the near future.

AdaCore has been deeply involved in the safety-critical sector for many years, through compiler and tool support and also through partnerships with other solution providers. One of our goals is to make it more efficient to achieve and demonstrate safety, security and reliability properties, and that’s the idea behind the Open-DO initiative: to increase the agility and the level of automation in producing and certifying safety-critical software.

AdaCore is also partnered with Altran Praxis for SPARK Pro, and with SoCheck for CodePeer. These tools are especially useful for safety-critical and high-security applications, and they nicely complement our GNAT Pro products. They are tightly integrated with GNAT Pro, which simplifies software development.

When I started working with Ada, one of its strongest attractions was the wide range of programming errors that were detected by the compiler. SPARK Pro and CodePeer go much further, preventing defects through construction and inspection respectively.

Any hobbies or outside interests that you’d like to share?

…I enjoy reading and traveling, and thanks to AdaCore I travel quite a bit. I also like practicing different sports (cycling, jogging, swimming, gym). After a day spent sitting in front of my computer, some physical activity is relaxing. I recently started experimenting with modeling technologies to develop control systems for robots. I use the LEGO MINDSTORMS, and it is really fun! My young daughter also appreciates my new hobby, but she is remarkably demanding in terms of functional requirements.

AdaCore Awarded Grant for Hi-Lite Project

Combines Testing, Static Analysis, and Formal Proofs

In March 2010 AdaCore was awarded a grant by French national and local government agencies to develop an innovative set of tools integrated with its GNAT Pro platform. AdaCore is leading a consortium of two research institutes (CEA-List and the ProVal team of INRIA) and four industrial companies (AdaCore, Altran, Astral and Thales Communications) in this effort. The project, named Hi-Lite, is starting in mid-2010 and will continue for three years.

Hi-Lite’s aim is to promote the use of formal methods in developing high-integrity software. It looses integrates formal proofs with testing and static analysis, thus allowing developers to combine different techniques around a common expression of properties and constraints. Hi-Lite’s focus on modularity allows a divide-and-conquer approach to large software systems and encourages early adoption by all programmers. By relying on only sound static analyses, Hi-Lite can assist industrial users who wish to apply the Formal Methods Supplement of the upcoming DO-178C avionics standard.

In short, the Hi-Lite project is completely based on Free Software. The project is structured as two different toolchains for Ada and C based on GNAT/GCC compilers (Ada and C), the CodePeer static analyzer (Ada), the SPARK verification toolset (Ada) and the Frama-C platform (C). The integration of these toolchains inside AdaCore IDEs will offer to the user a consistent way of dealing with Ada and C programs. In particular, mixed Ada/C programs can be verified against a common expression of properties and constraints.
GNAT Pro 6.3

This major release is available on more than fifty native and cross platforms comprising hundreds of different environments (variations of Ada run-time libraries and host/target Operating System versions). Highlights include:

- CodeRepos, a new add-on tool for automated code review and validation.
- C++ support as an option, for projects using C++ as well as Ada.
- Global tool improvements to the pretty printer (gnatplay), coding standard verifier (gnatchk), stack size analyzer (gnatstack), and the C and C++ binding generators.
- Specific tool improvements:
  - Unused dispatching subprogram elimination (gnatelim)
  - More flexible project handling
  - More efficient gnatmake and gnatbuil
  - Compiler and debugger enhancements
  - Many additional warnings
  - More flexibility in enabling/disabling warnings
  - Faster unbound symbol implementation
  - Removal of redundant run-time checks
- Support for Ada 2012 conditional expressions
- Better code generation (speed and size)
- More compact debugging information
- Improved interfacing with C++

The 6.3 release also includes the latest versions of the GNAT Programming Studio (GPS 4.4) and GNA TBench (2.4). GPS 4.4 is compatible with GNAT Pro versions 3.16.1 up to 6.3.

SPARK Pro 9.0

The latest version of SPARK Pro, a joint offering from AdaCore and Altair Praxis, is a major release with many enhancements:

- New information-flow verification for safety and security policies, such as Bell-LaPadula, based on integrity labeling of own variables.
- New SPARK 2005 language profile, including Mod, ‘Machine_Initialization, new reserved words, and the static semantics of “overriding”.
- Detection of dead statements, branches and paths in SPARK code, complementing the Simplifier and POOG.
- Cross Referencing annotations in GPS.
- Treatment of function annotation like procedure pre- and post-conditions. The annotations are subtitled in the caller’s VCS hypotheses, thus greatly improving the theorem prover’s effectiveness.
- A new output format for POOG designed to be both easier to read and easier to search automatically.
- Case checking, through a new Examiner switch that enforces consistent casing within code and annotations.

GPRbuild 1.4

The latest release of GPRbuild, a tool for constructing systems written in a combination of programming languages, offers a number of enhancements. Analysis is more precise, so GPRbuild is now much better at detecting implicit coupling between subprograms (no-indirect-imports). Performance is greatly improved on large projects, especially when remote disks are used, since the number of system calls has been significantly reduced. GPRbuild also supports new configurations including Apple Snow Leopard, LynuxWorks LynuxOS 5, and VSYSQ ELPOS.

- in the pipeline -

GNATStack

The GNATStack static stack analysis tool is being tightly integrated with GPS, making it easier for developers to use the tool and to visualize the stack usage information. GPS will gather the required data, launch GNATstack, and then display the worst-case call tree from any subprogram and annotate the subprogram with stack usage information.

GNATStack is also being enhanced to analyze object-oriented applications more precisely, automatically determining maximum stack usage on code that uses dynamic dispatching in both Ada and C++. A dispatching call challenges static analysis because the identity of the subprogram being invoked is not known until run time. GNATStack and the compiler are able to statically determine the subset of potential target primitive operations for every dispatching call. This will heavily reduce the analysis effort and will yield precise stack usage bounds on complex Ada/C++ code.

Webinar Schedule

Tuesday, April 27 / SPARK Pro 9.0

The Insight webinar series continues this Spring with a presentation by Robin McKenzie (Altair Praxis) on the new version of SPARK Pro, the AdaCore / Altair Praxis joint offering. The webinar discusses and demonstrates the new features of this major release and includes a question and answer session. To register, please visit www.adacore.com/home/products/gnatpro/webinars.

< academia corner >

Spotlighting a GAP Member

University of Virginia (USA)

At the University of Virginia, Ada lies at the core of a comprehensive approach to creating safety-critical applications. Dr. John Knight and his students, Xiang Yin, have created a practical approach to formal verification called Echo. In Echo verification, a program written in SPARK Ada is verified to conform to its SPARK annotations using the SPARK tools. The developer then uses automated Echo tools to simplify the annotated code and extract a specification in the PVS language (PVS is a specification and verification system from SRI). Finally, the extracted specification is shown to refine an original formal specification using the semi-automated PVS proof system. Echo’s strategy of splitting the formal verification process into the middle and attacking it from both sides dramatically reduces the effort needed to complete a formal verification, enabling Dr. Knight and his students to complete verification of systems as large as 10,000 lines of Ada code.

One project that has benefited from Ada and Echo verification is the University of Virginia’s LifeFlow artificial heart pump. Designed for the long-term (10–20 year) treatment of heart pump, this pump has a continuous-flow, axial design. The use of magnetic bearings and computational fluid dynamics simulation permits a streamlined path for blood flow. Compared with earlier pumps that used mechanical bearings, this flow path reduces the damage done to blood cells, thus reducing the potential for the formation of dangerous blood clots.

Control of the magnetic bearings is provided by a Freescale MPC5554 microcontroller executing control software written in SPARK Ada by Patrick Graydon and compiled using AdaCore’s GNAT Pro High-Integrity Edition compiler. The control software runs natively on the microcontroller with no operating system, limiting the software base that must be verified for this critical application. Comprehensive Echo formal verification complements functional testing to Modified Condition / Decision Coverage (MCDC), providing high confidence that the magnetic bearing controller is free of defects, as can practically be achieved.

For further information about the Echo approach and the LifeFlow project, please see dependability.cs.virginia.edu/info/Echo and drac.mae.virginia.edu/fileFlow/.

AdaCore has been providing software development solutions for high-integrity systems for many years. How do you see the marketplace evolving, and what is AdaCore doing to meet the new demands?

AdaCore has been providing software development solutions for high-integrity systems for many years. How do you see the marketplace evolving, and what is AdaCore doing to meet the new demands?

Tell us about your background and how you came to be involved with Ada and AdaCore. What is your current role?

I discovered Ada as a student at the Technical University of Madrid, thanks to Professors Juan Antonio de la Puente and Alejandro Alonso. My first major Ada project involved porting the University of Virginia life-flow pump system to bareboard PICs, and I was fascinated by the embedded world where you control everything that is executing on your system. Then, during my Ph.D. work, I helped implement a run-time library supporting the Ravenscar profile for space processors. That project tightened my relationship with AdaCore and subsequently led to an offer to join their Paris office. This was an excellent career opportunity, and my wife liked the prospect of living in Paris, so saying “yes” was an easy decision.

Here at AdaCore I’m working on applied research for safety-critical embedded real-time systems. Projects include adapting Ravenscar towards new functionalities and targets, and exploring qualification and certification solutions for high-integrity software. I also work on GNAT technology development, and I’ve recently been implementing some enhancements to GNATStack.

I see an encouraging increase in the number of new projects focusing on safety aspects. Systems are growing in size and complexity—not only in our traditional markets like aerospace but also in others such as automotive. With the safety and economic implications of failures in these systems, I expect high-integrity methodologies to be much more widely embraced in the near future.

AdaCore has been deeply involved in the safety-critical world for many years, through compiler and tool support and also through partnerships with other solution providers. One of our goals is to make it more efficient to achieve and demonstrate safety, security and reliability properties, and that’s the idea behind the Open-DO initiative: to increase the agility and the level of automation in producing and certifying safety-critical software.

AdaCore is also partnered with Altair Praxis for SPARK Pro, and with SoftCheck for CodePeer. These tools are especially useful for safety-critical and high-security applications, and they nicely complement our GNAT Pro products. They are tightly integrated with GNAT Pro, which simplifies software development.

When I started working with Ada, one of its strongest attractions was the wide range of programming errors that were detected by the compiler. SPARK Pro and CodePeer go much further, preventing defects through construction and inspection respectively.

Any hobbies or outside interests that you’d like to share in?

I enjoy reading and traveling, and thanks to AdaCore I travel quite a bit. I also like practicing different sports (cycling, jogging, swimming, gym). After a day spent sitting in front of my computer, some physical activity is relaxing. I recently started experimenting with modeling technologies to develop control systems for robots. I use the LEGO MINDSTORMs, and it is really fun! My young daughter also appreciates my new hobby, but she is remarkably demanding in terms of functional requirements.

Interview with José Ruiz
Senior Software Engineer, AdaCore EU

In March 2010 AdaCore was awarded the French national and local government agencies to develop an innovative set of tools integrated with its GNAT Pro platform. AdaCore is leading a consortium of two research institutes (CEA-List and the PrVoLab team of INRIA) and four industrial companies (AdaCore, Altair, Astramus and Thales Communications) in this effort. The project, named Hi-Lite, is starting in mid-2010 and will continue for three years.

Hi-Lite’s aim is to promote the use of formal methods in developing high-integrity software. It loosely integrates formal proofs with testing and static analysis, thus allowing developers to combine different techniques around a common expression of properties and constraints. Hi-Lite’s focus on modularity allows a divide-and-conquer approach to large software systems and encourages early adoption by all programmers. By relying only on sound static analyses, Hi-Lite can assist industrial users who wish to apply the formal Methods Supplement of the upcoming DO-178C avionics standard.

Hi-Lite is completely based on Free Software. The project is structured as two different toolchains for Ada and C based on GNAT/GCC compilers (Ada and C), the CodePeer static analyzer (Ada), the SPARK verification toolset (Ada) and the Frama-C platform (C). The integration of these toolchains inside AdaCore IDEs will offer to the user a consistent way of dealing with Ada and C programs. In particular, mixed Ada/C programs can be verified against a common expression of properties and constraints.

AdaCore Awarded Grant for Hi-Lite Project

Combines Testing, Static Analysis, and Formal Proofs

In March 2010 AdaCore was awarded by French national and local government agencies to develop an innovative set of tools integrated with its GNAT Pro platform. AdaCore is leading a consortium of two research institutes (CEA-List and the PrVoLab team of INRIA) and four industrial companies (AdaCore, Altair, Astramus and Thales Communications) in this effort. The project, named Hi-Lite, is starting in mid-2010 and will continue for three years.

Hi-Lite’s aim is to promote the use of formal methods in developing high-integrity software. It loosely integrates formal proofs with testing and static analysis, thus allowing developers to combine different techniques around a common expression of properties and constraints. Hi-Lite’s focus on modularity allows a divide-and-conquer approach to large software systems and encourages early adoption by all programmers. By relying only on sound static analyses, Hi-Lite can assist industrial users who wish to apply the formal Methods Supplement of the upcoming DO-178C avionics standard.

Hi-Lite is completely based on Free Software. The project is structured as two different toolchains for Ada and C based on GNAT/GCC compilers (Ada and C), the CodePeer static analyzer (Ada), the SPARK verification toolset (Ada) and the Frama-C platform (C). The integration of these toolchains inside AdaCore IDEs will offer to the user a consistent way of dealing with Ada and C programs. In particular, mixed Ada/C programs can be verified against a common expression of properties and constraints.
Ada 2012 Nearing Completion

Next Version of Language Standard Offers Numerous Enhancements

As part of the natural evolution of the language design, a new version of the Ada standard is nearing completion. Referring to Ada 2012, this is an upwards-compatible increment to Ada 2005. A number of new features are currently under consideration, including:

- Improved support for specifying assertions (membership predicates for subtypes, pre- and postconditions for subprograms, invariants for packages and types, global in-out annotations);
- Improved support for real-time and concurrent programming (multiprocessor Ravenscar, barriers, task/processor affinities, task-safe queues);
- Bounded forms of the container packages appropriate in applications that cannot use dynamic storage allocation or controlled types;
- Improved support for iterating over the elements of a container or array;
- More flexible forms of expressions (if-expressions, case-expressions, quantified expressions, more general membership tests);
- Improved support for controlling visibility of names (use all type, integrated packages);
- Region-based memory management via subpools of storage pools;
- "in out" and "out" modes for functions;
- New uses for incomplete types (to introduce a private type, as a parameter or result type, as a generic formal parameter).

For details, please see www.ada-auth.org/ai05-summary.html.

As their design firms up, many of these features are being prototyped in the GNAT technology (for example if- and case-expressions), allowing customers to gain early experience. With this phased-in approach, comprehensive support for Ada 2012 is expected soon after the final language definition is approved.

Open-DO Update

Launched in early 2009, the Open-DO initiative promotes using open source software and lean / agile methodology in developing and certifying high-integrity systems. This year’s Open-DO conference took place in Paris on March 11 and focused on how to combine formal methods with agile development. Notable speakers included Niel White (Deltanet) and Dr. Jérôme Lambourg, José Ruiz, and Ed Schonberg.

AdaCore is a sponsor of this event.

CodéPeer Launched

The CodéPeer source code analyzer / reviewer for Ada is now available. This tool identifies constructs that are likely to lead to run-time errors such as buffer overflows, and it flags legal but suspicious code indicating logic errors. With surpassing typical static analysis tools, CodéPeer also produces a detailed analysis of each subprogram, including pre- and postconditions. Previous bugs and vulnerabilities can thus be traced immediately.

CodéPeer can be used productively during program development and upgrade, to prevent errors being introduced or augmented. A systematic code inspection process and thus maximizes the efficiency of human review. It can also be used efficiently on existing codebases, to detect and remove latent bugs.

CodéPeer analyzes Ada programs for a wide range of flaws including pointer misuse, buffer overflows, and program verification, and it has recently produced a detailed analysis of a怀疑 that the component is faulty.

Aerospace and Defense Technical Forums in the Spring

AdaCore has set up an infrastructure for producing DO-178C ready qualification, and three others adapt the core document guidance when specific needs are encountered. DO-178B, with a number of clarifications and a few minor corrections. The major change is the inclusion of several supplements. The core documents deal with tool qualification, and several others adapt the core document guidance when specific technologies are used: Model-Based Development, Object-Oriented Technologies, and Formal Methods. AdaCore has been participating in the DO-178C revision process, with Dr. Cyrilie Coram contributing to the Object-Oriented Technologies subgroup.

AdaCore has set up an infrastructure for producing DO-178C ready qualification material for GNATcross, GNATStack, and tools that support the "substantially improved" project for structural coverage analysis up to level A. If you have specific questions about DO-178C related to AdaCore technology, do not hesitate to ask them through your GNAT Tracker account.