APRON: Analyse de PRogrammes Numérique

Projet 2004

François Irigoin

École des Mines de Paris - Centre de Recherche en Informatique

17 novembre 2004

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

Quelles sont les questions posées ?

- Les tableaux sont-ils bien utilisés (*buffer overflows*) ?
- Les variables sont-elles initialisées ?
- L'aliasing peut-il créer des problèmes de portabilité ?
- La boucle critique s'exécute-t-elle dans le temps alloué ?
- Peut-on garantir l'absence d'exceptions ?
- Ce programme parallèle est-il déterministe ?
- ...

L'analyse statique de programmes, les défis d'APRON

- temps de l'analyse ?
- magnitude ?
- espace ?
- précision des analyses :
  - nombre de points de contrôle ?
  - connaissance de l'histoire du calcul ?
  - qualité des points fixes ?
- domaines de valeurs :
  - calculs flottants ?
  - structures de données ?
  - valeurs gardées ?

L'analyse statique de programmes, les défis d'APRON

- temps de l'analyse ?
- magnitude ?
- espace ?
- précision des analyses :
  - nombre de points de contrôle ?
  - connaissance de l'histoire du calcul ?
  - qualité des points fixes ?
- domaines de valeurs :
  - calculs flottants ?
  - structures de données ?
  - valeurs gardées ?

L'analyse statique de programmes, les défis d'APRON

- temps de l'analyse ?
- magnitude ?
- espace ?
- précision des analyses :
  - nombre de points de contrôle ?
  - connaissance de l'histoire du calcul ?
  - qualité des points fixes ?
- domaines de valeurs :
  - calculs flottants ?
  - structures de données ?
  - valeurs gardées ?

L'analyse statique de programmes, les défis d'APRON

- temps de l'analyse ?
- magnitude ?
- espace ?
- précision des analyses :
  - nombre de points de contrôle ?
  - connaissance de l'histoire du calcul ?
  - qualité des points fixes ?
- domaines de valeurs :
  - calculs flottants ?
  - structures de données ?
  - valeurs gardées ?

L'analyse statique de programmes, les défis d'APRON

- temps de l'analyse ?
- magnitude ?
- espace ?
- précision des analyses :
  - nombre de points de contrôle ?
  - connaissance de l'histoire du calcul ?
  - qualité des points fixes ?
- domaines de valeurs :
  - calculs flottants ?
  - structures de données ?
  - valeurs gardées ?

L'analyse statique de programmes, le périmètre

- nature du programme à analyser :
  - taille du programme : 100 à 500 000 LOC
  - nombre de procédures : 1000, 2000 ?
  - les types de données : flottants, booléens, entiers, structures
- ressources disponibles :
  - espace nécessaire à l'analyse
  - temps d'exécution de l'analyse
  - précision numérique de l'analyse (32, 64, 128 bits, gmp ?)
- résultats attendus :
  - preuve de propriétés critiques
  - absence de certaines erreurs à l'exécution
  - localisation d'erreurs
- précision des analyses :
  - nouveaux domaines abstraits,
  - adaptativité,
  - points fixes

L'analyse statique de programmes, le périmètre

- nature du programme à analyser :
  - taille du programme : 100 à 500 000 LOC
  - nombre de procédures : 1000, 2000 ?
  - les types de données : flottants, booléens, entiers, structures
- ressources disponibles :
  - espace nécessaire à l'analyse
  - temps d'exécution de l'analyse
  - précision numérique de l'analyse (32, 64, 128 bits, gmp ?)
- résultats attendus :
  - preuve de propriétés critiques
  - absence de certaines erreurs à l'exécution
  - localisation d'erreurs
- précision des analyses :
  - nouveaux domaines abstraits,
  - adaptativité,
  - points fixes

L'analyse statique de programmes, le périmètre

- nature du programme à analyser :
  - taille du programme : 100 à 500 000 LOC
  - nombre de procédures : 1000, 2000 ?
  - les types de données : flottants, booléens, entiers, structures
- ressources disponibles :
  - espace nécessaire à l'analyse
  - temps d'exécution de l'analyse
  - précision numérique de l'analyse (32, 64, 128 bits, gmp ?)
- résultats attendus :
  - preuve de propriétés critiques
  - absence de certaines erreurs à l'exécution
  - localisation d'erreurs
- précision des analyses :
  - nouveaux domaines abstraits,
  - adaptativité,
  - points fixes

L'analyse statique de programmes, le périmètre

- nature du programme à analyser :
  - taille du programme : 100 à 500 000 LOC
  - nombre de procédures : 1000, 2000 ?
  - les types de données : flottants, booléens, entiers, structures
- ressources disponibles :
  - espace nécessaire à l'analyse
  - temps d'exécution de l'analyse
  - précision numérique de l'analyse (32, 64, 128 bits, gmp ?)
- résultats attendus :
  - preuve de propriétés critiques
  - absence de certaines erreurs à l'exécution
  - localisation d'erreurs
- précision des analyses :
  - nouveaux domaines abstraits,
  - adaptativité,
  - points fixes

Les approches possibles, autres projets

- interprétation abstraite
- Model Checking
- Analyseurs : Stanford, Berkeley
- Programmer Productivity Research Center (Microsoft)
- logiciels critiques embarqués
- approches adaptatives

Les approches possibles, autres projets

- interprétation abstraite
- Model Checking
- Analyseurs : Stanford, Berkeley
- Programmer Productivity Research Center (Microsoft)
- logiciels critiques embarqués
- approches adaptatives

Les approches possibles, autres projets

- interprétation abstraite
- Model Checking
- Analyseurs : Stanford, Berkeley
- Programmer Productivity Research Center (Microsoft)
- logiciels critiques embarqués
- approches adaptatives

Les approches possibles, autres projets

- interprétation abstraite
- Model Checking
- Analyseurs : Stanford, Berkeley
- Programmer Productivity Research Center (Microsoft)

- logiciels critiques embarqués
- approches adaptatives

Les approches possibles, autres projets

- interprétation abstraite
- Model Checking
- Analyseurs : Stanford, Berkeley
- Programmer Productivity Research Center (Microsoft)

- logiciels critiques embarqués
- approches adaptatives

Les approches possibles, autres projets

- interprétation abstraite
- Model Checking
- Analyseurs : Stanford, Berkeley
- Programmer Productivity Research Center (Microsoft)

- logiciels critiques embarqués
- approches adaptatives

L'interprétation abstraite : un rappel ?

- modélisation de l'environnement (facultatif)
- modélisation des valeurs et de l'état
- modélisation des commandes (facultatif)
- dérivation automatique et correcte du modèle
- résolution du système d'équations modélisant le programme
- décidabilité : approximations

L'interprétation abstraite : un rappel ?

- modélisation de l'environnement (facultatif)
- modélisation des valeurs et de l'état
- modélisation des commandes (facultatif)
- dérivation automatique et correcte du modèle
- résolution du systéme d'équations modélisant le programme
- décidabilité, approximations

L'interprétation abstraite : un rappel ?

- modélisation de l'environnement (facultatif)
- modélisation des valeurs et de l'état
- modélisation des commandes (facultatif)
- dérivation automatique et correcte du modèle
- résolution du systéme d'équations modélisant le programme
- décidabilité : approximations

L'interprétation abstraite : un rappel ?

- modélisation de l'environnement (facultatif)
- modélisation des valeurs et de l'état
- modélisation des commandes (facultatif)
- dérivation automatique et correcte du modèle
- résolution du systéme d'équations modélisant le programme
- décidabilité : approximations

L'interprétation abstraite : un rappel ?

- modélisation de l'environnement (facultatif)
- modélisation des valeurs et de l'état
- modélisation des commandes (facultatif)
- dérivation automatique et correcte du modèle
- résolution du systéme d'équations modélisant le programme
- décidabilité : approximations

L'interprétation abstraite : un rappel ?

- modélisation de l'environnement (facultatif)
- modélisation des valeurs et de l'état
- modélisation des commandes (facultatif)
- dérivation automatique et correcte du modèle
- résolution du systéme d'équations modélisant le programme
- décidabilité : approximations

Les partenaires d'APRON

- Patrick Cousot, ENS (LIENS)
- Radhia Cousot, Ecole polytechnique (STIX)
- Nicolas Halbwachs, VERIMAG
- François Irigoin, Ecole des mines de Paris(CRI)
- Bertrand Jeannet, IRISA (VERTECS)

Les partenaires d'APRON

- Patrick Cousot, ENS (LIENS)
- Radhia Cousot, Ecole polytechnique (STIX)
- Nicolas Halbwachs, VERIMAG
- François Irigoin, Ecole des mines de Paris(CRI)
- Bertrand Jeannet, IRISA (VERTECS)

Les partenaires d'APRON

- Patrick Cousot, ENS (LIENS)
- Radhia Cousot, Ecole polytechnique (STIX)
- Nicolas Halbwachs, VERIMAG
- François Irigoin, Ecole des mines de Paris(CRI)
- Bertrand Jeannet, IRISA (VERTECS)

Les partenaires d'APRON

- Patrick Cousot, ENS (LIENS)
- Radhia Cousot, Ecole polytechnique (STIX)
- Nicolas Halbwachs, VERIMAG
- François Irigoin, Ecole des mines de Paris(CRI)
- Bertrand Jeannet, IRISA (VERTECS)

Les partenaires d'APRON

- Patrick Cousot, ENS (LIENS)
- Radhia Cousot, Ecole polytechnique (STIX)
- Nicolas Halbwachs, VERIMAG
- François Irigoin, Ecole des mines de Paris(CRI)
- Bertrand Jeannet, IRISA (VERTECS)

Les partenaires d'APRON

- Patrick Cousot, ENS (LIENS)
- Radhia Cousot, Ecole polytechnique (STIX)
- Nicolas Halbwachs, VERIMAG
- François Irigoin, Ecole des mines de Paris(CRI)
- Bertrand Jeannet, IRISA (VERTECS)

Les outils utilisés par les partenaires d'APRON

- ASTREE, l'analyseur de code C développé au LIENS et au STIX
- PIPS, un analyseur interprocédural modulaire développé au CRI
- NBAC, un analyseur d'applications LUSTRE développé à l'IRISA et à VERIMAG

Les outils utilisés par les partenaires d'APRON

- ASTREE, l'analyseur de code C développé au LIENS et au STIX
- PIPS, un analyseur interprocédural modulaire développé au CRI
- NBAC, un analyseur d'applications LUSTRE développé à l'IRISA et à VERIMAG

Les outils utilisés par les partenaires d'APRON

- ASTREE, l'analyseur de code C développé au LIENS et au STIX
- PIPS, un analyseur interprocédural modulaire développé au CRI
- NBAC, un analyseur d'applications LUSTRE développé à l'IRISA et à VERIMAG

Les outils utilisés par les partenaires d'APRON

- ASTREE, l'analyseur de code C développé au LIENS et au STIX
- PIPS, un analyseur interprocédural modulaire développé au CRI
- NBAC, un analyseur d'applications LUSTRE développé à l'IRISA et à VERIMAG

Première partie
Description du projet

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les nouveaux domaines abstraits

- Les nombres flottants
- Les calculs non linéaires
- Les domaines gardés (abstraction logico-numérique)
- Les structures de données (abstraction symbolico-numérique)
- Les produits de domaines abstraits
- Information d'exactitude
- Abstraction robuste, opérateurs dégradés

Les abstractions du contrôle

- partitionnement de traces
- partitionnement dynamique

Les abstractions du contrôle

- partitionnement de traces
- partitionnement dynamique

Résolution itérative

- stratégie d'itération pour les analyses en avant et en arrière
- amélioration(s) de l'élargissement
- accélération de point fixe

Résolution itérative

- stratégie d'itération pour les analyses en avant et en arrière
- amélioration(s) de l'élargissement
- accélération de point fixe

Résolution itérative

- stratégie d'itération pour les analyses en avant et en arrière
- amélioration(s) de l'élargissement
- accélération de point fixe

Analyse interprocédurale modulaire

- inlining
- temps d'analyse linéaire avec la taille du programme
- précision de l'abstraction des procédures ?
- adaptativité et clônage
- appels récursifs

Analyse interprocédurale modulaire

- inlining
- temps d'analyse linéaire avec la taille du programme
- précision de l'abstraction des procédures ?
- adaptativité et clônage
- appels récursifs

Analyse interprocédurale modulaire

- inlining
- temps d'analyse linéaire avec la taille du programme
- précision de l'abstraction des procédures ?
- adaptativité et clônage
- appels récursifs

Analyse interprocédurale modulaire

- inlining
- temps d'analyse linéaire avec la taille du programme
- précision de l'abstraction des procédures ?
- adaptativité et clônage
- appels récursifs

Analyse interprocédurale modulaire

- inlining
- temps d'analyse linéaire avec la taille du programme
- précision de l'abstraction des procédures ?
- adaptativité et clônage
- appels récursifs

Le *slicing* abstrait

- ne pas tout analyser
- précision ?
- *slicing* du contrôle
- *slicing* des données

Le *slicing* abstrait

- ne pas tout analyser
- précision ?
- *slicing* du contrôle
- *slicing* des données

Le *slicing* abstrait

- ne pas tout analyser
- précision ?
- *slicing* du contrôle
- *slicing* des données

Le *slicing* abstrait

- ne pas tout analyser
- précision ?
- *slicing* du contrôle
- *slicing* des données

Le *slicing* abstrait

- ne pas tout analyser
- précision ?
- *slicing* du contrôle
- *slicing* des données

Au niveau fondamental

- de nouveaux domaines abstraits
  - flottants
  - non-linéaires
  - logico-numériques
  - symbolico-numériques
  - avec partitionnement de trace
  - avec partitionnement dynamique
  - avec produits de domaines
- de nouvelles stratégies itératives avec élargissement et accélération
- des techniques de *slicing* abstrait mais précis

Au niveau fondamental

- de nouveaux domaines abstraits
  - flottants
  - non-linéaires
  - logico-numériques
  - symbolico-numériques
  - avec partitionnement de trace
  - avec partitionnement dynamique
  - avec produits de domaines
- de nouvelles stratégies itératives avec élargissement et accélération
- des techniques de *slicing* abstrait mais précis

Au niveau fondamental

- de nouveaux domaines abstraits
  - flottants
  - non-linéaires
  - logico-numériques
  - symbolico-numériques
  - avec partitionnement de trace
  - avec partitionnement dynamique
  - avec produits de domaines
- de nouvelles stratégies itératives avec élargissement et accélération
- des techniques de *slicing* abstrait mais précis

Au niveau technologique

- des interfaces communes
- l'adaptation de bibliothèques existantes à ces interfaces
- le développement de nouvelles bibliothèques
- la prise en compte de la généricité dans les outils existants
- des comparaisons entre domaines abstraits

Au niveau technologique

- des interfaces communes
- l'adaptation de bibliothèques existantes à ces interfaces
- le développement de nouvelles bibliothèques
- la prise en compte de la généricité dans les outils existants
- des comparaisons entre domaines abstraits

Au niveau technologique

- des interfaces communes
- l'adaptation de bibliothèques existantes à ces interfaces
- le développement de nouvelles bibliothèques
- la prise en compte de la généricité dans les outils existants
- des comparaisons entre domaines abstraits

Au niveau technologique

- des interfaces communes
- l'adaptation de bibliothèques existantes à ces interfaces
- le développement de nouvelles bibliothèques
- la prise en compte de la généricité dans les outils existants
- des comparaisons entre domaines abstraits

Au niveau technologique

- des interfaces communes
- l'adaptation de bibliothèques existantes à ces interfaces
- le développement de nouvelles bibliothèques
- la prise en compte de la généricité dans les outils existants
- des comparaisons entre domaines abstraits

Au niveau expérimental

- PIPS avec octogones : impact de la précision sur les résultats ?
- PIPS avec librairie polyédrique de VERIMAG : vitesse ?
- Amélioration des outils sur les benchmarks APRON

Au niveau expérimental

- PIPS avec octogones : impact de la précision sur les résultats ?
- PIPS avec librairie polyédrique de VERIMAG : vitesse ?
- Amélioration des outils sur les benchmarks APRON

Au niveau expérimental

- PIPS avec octogones : impact de la précision sur les résultats ?
- PIPS avec librairie polyédrique de VERIMAG : vitesse ?
- Amélioration des outils sur les benchmarks APRON

Deuxième partie
Organisation du projet

Schéma général du projet

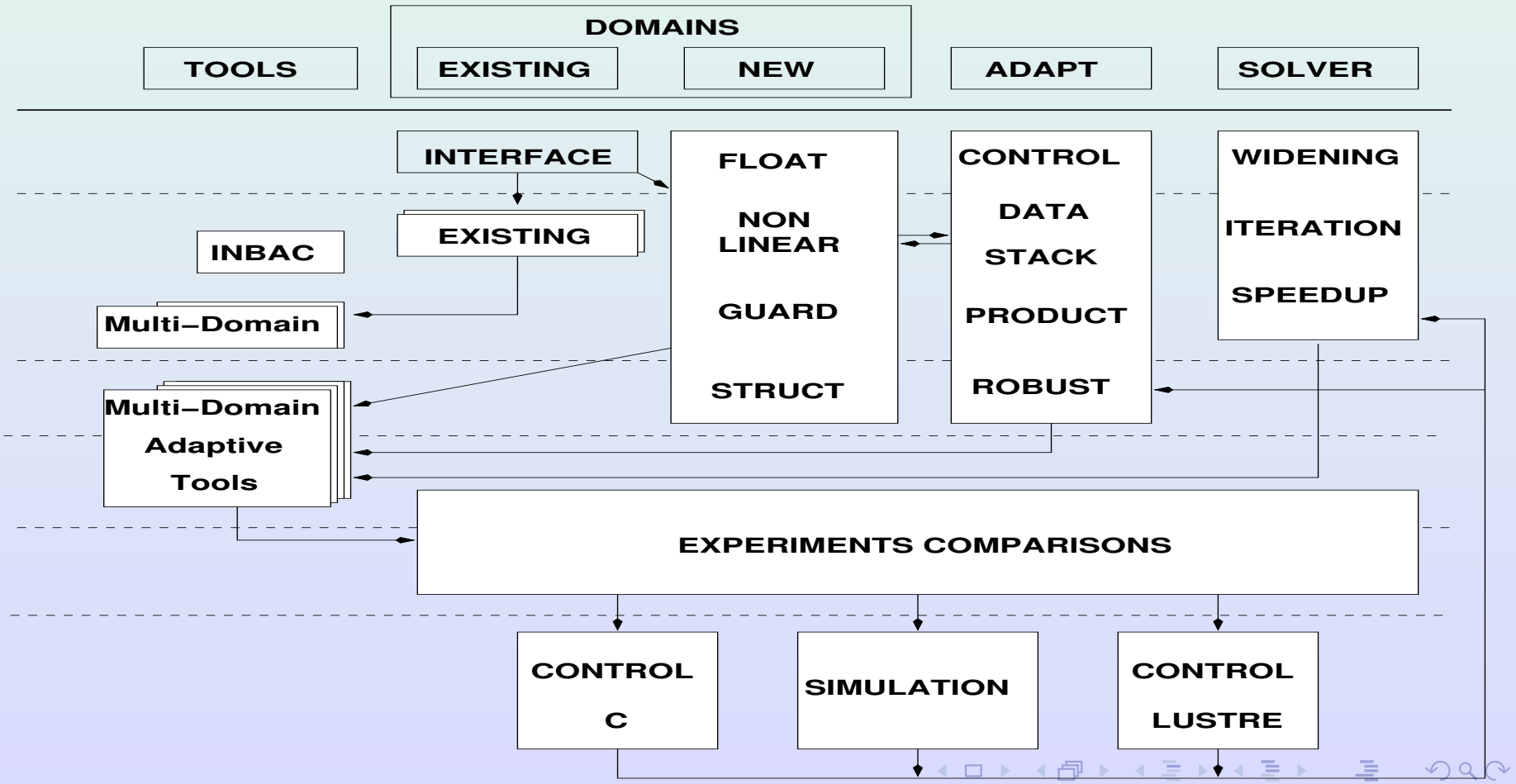
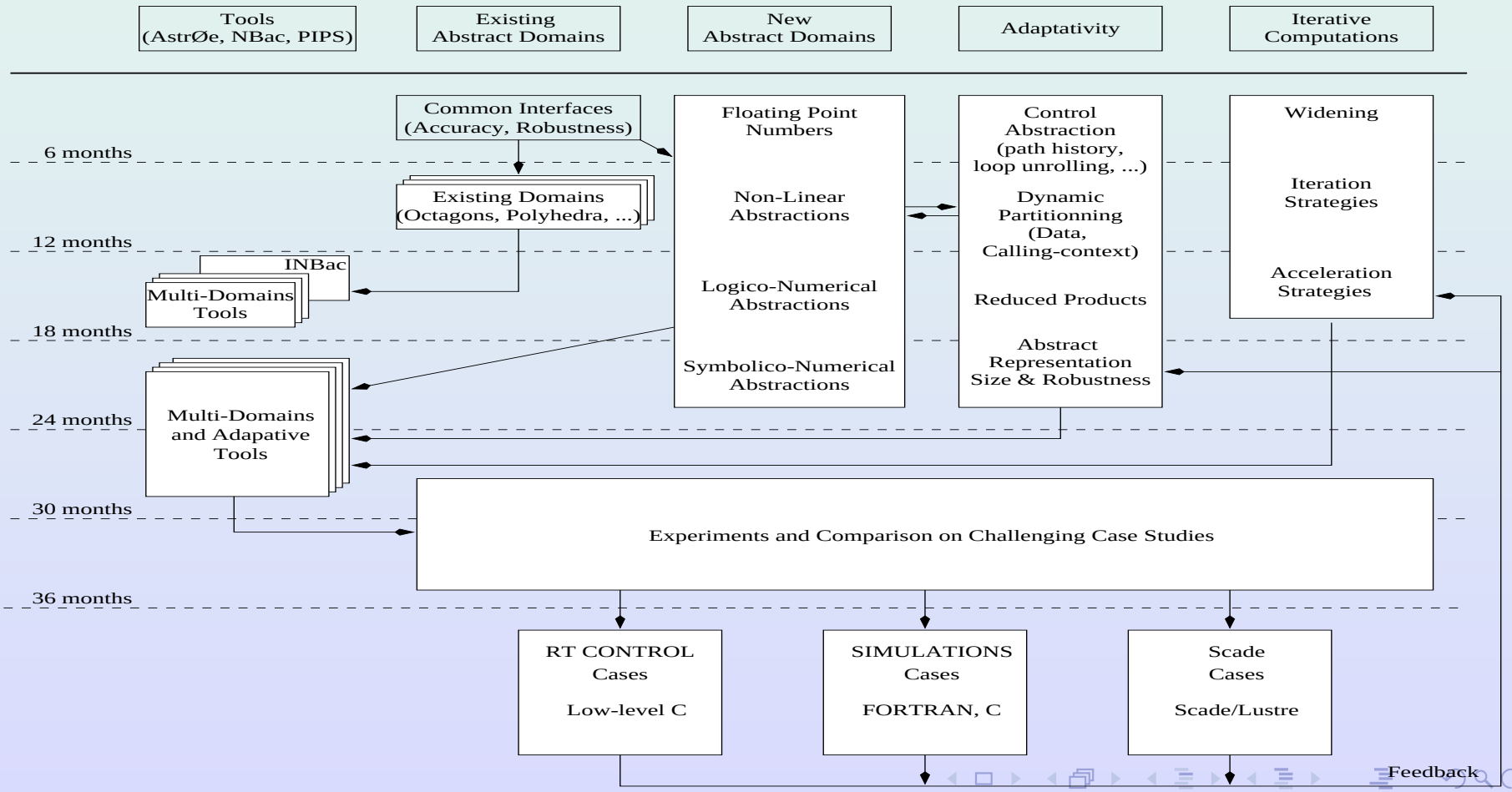


Schéma détaillé du projet



Planning du projet

- réunion de lancement : 28 octobre 2004
- 6 mois :
  - interfaces génériques, avec support pour exactitude et robustesse
  - définition des benchmarks
- 12 mois :
  - bibliothèques C pour les domaines existants avec la nouvelle interface
  - nouveaux algorithmes pour élargissement, itération, accélération et partitionnement dynamique
- 18 mois :
  - bibliothèques C pour les nouveaux domaines abstraits
  - version multidomaine de NBAC (polyèdre, octogone, intervalle)
  - nouvel outil interprocédural, INBAC

Planning du projet (suite)

- 24 mois :
  - intégration de la nouvelle API dans les outils existants pour certains domaines
  - nouveaux algorithmes (slicing, élargissement, accélération, partitionnement)
  - algorithmes adaptatifs : partitionnements dynamiques, partitionnement de traces, partitionnement du contrôle, listes de polyèdres
- 30 mois :
  - INBAC and NBAC avec produits cartésiens et réduits
  - PIPS avec un nouveau domaine abstrait et des algorithmes adaptatifs partitionnement de traces, partitionnement du contrôle, listes de polyèdres
- 36 mois :
  - résultats expérimentaux avec les nouveaux domaines et les nouvelles strategies de resolution

Conclusion

- des objectifs ambitieux : fondamentaux, technologiques et expérimentaux
- mais largement découplés
- utilisation continue des retours expérimentaux
- une vraie collaboration
- un impact industriel : complexité des controleurs temps-réel, temps de développement

Questions & Remarques