科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月 １６ 日現在

機関番号：３２６８９
研究種目：基盤研究(B)
研究期間：2011～2013
課題番号：２３３０００１１

研究課題名（和文）高性能検証系を統合した高水準モデリング言語処理系の構築

研究課題名（英文）Implementations of high-level modeling languages that integrate high-performance verifiers

研究代表者
上田　和紀（Ueda, Kazunori）

早稲田大学・理工学術院・教授

研究者番号：１０２５７２０６

交付決定額（研究期間全体）：（直接経費）　　15,500,000円、（間接経費）　　4,650,000円

研究成果の概要（和文）：自然系や記号系，および両者が混在するサイバーフィジカルシステムのモデリングと検証技術は今後ますます重要性を増すと期待される．本研究では，グラフや集合，方程式や不等式といった，情報学の枠にとどまらない高度に一般的な概念に基づく高水準モデリング言語とそれを用いた検証技術の可能性を，実行系と検証系を統合した複数の処理系を具体的に構築することによって示した．本研究開発によって，グラフ書換え言語LMNtalの処理系はハイパーグラフ書換え機能を備えた並列モデル検査器へと進化し，ハイブリッド制約言語HydLaの処理系は不確定性をもつハイブリッドシステムの非決定的記号実行系へと進化した．

研究成果の概要（英文）：Modeling and verification technologies of natural, symbolic and cyber-physical systems are becoming increasingly important. The aim of this research was to demonstrate the viability of high-level modeling languages based on mathematical notions such as graphs, sets, equations and inequations whose generality goes far beyond Computer Science. To achieve this goal, we constructed two publicly available language implementations that integrate runtime systems and verifiers. One of them is an implementation of the graph rewriting language LMNtal, which has now evolved into a parallel model checker with hypergraph rewriting capabilities; the other is an implementation of the hybrid constraint language HydLa, which has evolved into a non-deterministic symbolic execution system for hybrid systems with uncertainties.

研究分野：情報学

科研費の分科・細目：計算基盤・ソフトウェア

キーワード：高水準モデリング言語　言語処理系　モデル検査　ハイブリッドシステム　並列処理

１．研究開始当初の背景

研究代表者らは非手続き型の高水準言語の設計と実装に長年従事し，2002 年からは並行制約プログラミングと多重集合概念をもつ多数の理論計算モデルとを統合する言語モデル LMNtal と 10 万行規模の処理系を構築してきた．また 2008 年からは系の挙動が連続変化と離散変化の両方を示すハイブリッドシステムのための並行制約言語 HydLa を提案し処理系を試作してきた．

この間，形式検証技術としてのモデル検査技術が大きな進歩と普及を遂げてきたが，モデル検査ツールで使われるモデリング言語の多くは記述力の点でプログラミング言語に劣っており，高水準言語を用いたモデル検査系の実現には，性能等の観点から解決すべき多くの技術課題が残されていた．またハイブリッドシステムにおいては，高水準言語の設計および実装技術は緒についたばかりであり，特に形式検証への展開を視野に入れた高信頼シミュレーション技術が大きな技術課題であった．

２．研究の目的

手続き型高水準言語の今後の適用分野として，自然系や記号系，および両者が混在するサイバーフィジカルシステムのモデリングと検証が重要性を増すと期待される．本研究では，高水準モデリング言語を用いた検証の高性能高機能化のために，並行性と非決定性をもつ言語の理論と実践に多くの蓄積をもつ研究代表者，システム検証技術に多くの蓄積をもつ研究分担者，および制約処理技術に蓄積をもつ連携研究者の知見を総合して，これまで開発してきた高水準言語を研究の基盤に据え，従来の実行系に高性能・高機能検証機能を統合した新たな処理系を構築する．

具体的には，

(a) 高度なデータ構造を持つモデリング言語の高性能並列モデル検査系．
(b) 高水準ハイブリッド言語のための並列検証系

の研究開発を同時に推進することによって高性能検証技術の交流と融合を促し，次世代の記述・検証体系に向けての新たな枠組を模索する．

３．研究の方法

本研究は，宣言型言語の設計と処理系開発に多くの経験をもつ研究代表者が全体を統括し，研究代表者のグループで培ってきた高水準モデリング言語とその処理系を高性能検証系へと発展させるべく，必要な要素技術を多方面から開発する．本グループは，教員と高いプログラミング能力をもつ学生とからなるチームが一致協力して，大規模な言語処理系を構築し長期にわたって継続的に発展させる経験とノウハウを蓄積している．

研究分担者は，これまで独自に培ってきた検証における抽象化技術と検証問題記述経験をさらに発展させつつ，その知見を本研究開発に統合する．さらに，研究代表者グループとの討議に継続的に参画してきた細部博史，および，2009 年度まで研究代表者の研究室で非線形ハイブリッドシステムの高信頼計算技術を開拓してきた石井大輔が，連携研究者として常時参加して，制約技術および区間計算技術の観点から研究開発に参画する．

４．研究成果

実行系と検証系を統合した高水準モデリング言語とその処理系の研究開発を，グラフ書換えに基づくモデリング言語 LMNtal とその実行系 slim，および制約概念に基づくハイブリッドシステム記述言語 HydLa とその実行系 Hyrose の二つを軸に推進して，以下の研究開発成果を得た．

(1) LMNtal のハイパーグラフ書換えモデルへの拡張

1 対 1 リンクに基づくグラフ構造は多くのプログラミング言語が備えるリストや木構造と比べて高い表現力をもつが，1 個以上任意個の節点間の接続を許すハイパーリンクを備えたハイパーグラフは，モデリング言語にさらに高い表現力をもたらす．そこで，ハイパーグラフ書換えのための言語機能を，既存の言語機能との整合性を保ちつつ LMNtal に導入するとともに LMNtal 抽象機械を拡張して slim に新機能を実装し，さらにモデル検査に必要な slim の状態空間構築機能をハイパーグラフ書換えに対応させた．

実装した機能の有効性を確認するために，制約プログラミング言語 CHR (Constraint Handling Rules)，並行計算モデル BRS (Bigraphical Reactive Systems)，純粋ラムダ計算，多相型推論系を含む多様な計算モデルや形式体系のエンコードと動作確認を行った．

(2) LMNtal 実行系の並列モデル検査器への発展

LMNtal 実行系 slim がもつ状態空間構築およびモデル検査の性能を大幅に向上すべく，共有メモリ並列計算機向けの並列化を実現した．グラフ書換えの差分情報を用いた状態展開の最適化，状態の圧縮表現，ヒューリスティクスを導入したグラフ同型性判定，stack slicing および work stealing に基づく低い並列化オーバーヘッドの状態空間構築管理などの多くの工夫よって，48 コア並列計算機上で，グラフ書換えモデル検査の実行時間のほとんどを占める状態空間構築処理に対して，平均約 31 倍（34 例題）の速度向上を達成した（図１）．

また，反例（受理サイクル）をもつ問題における状態空間構築コストを削減すべく，

on-the-fly 性能に優れるが並列効果の高くない Nested DFS アルゴリズムとその逆の特性をもつ MAP アルゴリズムを組み合わせた新たな並列モデル検査アルゴリズムを提案し実装した．

さらに，本並列モデル検査器を拡張してリアルタイムシステムのモデル検査器や組合せ最適化の並列求解系が構築できることを実証的に確認した．

本研究終了時点で，slim モデル検査器は数億状態のモデルの検証能力を実現している．

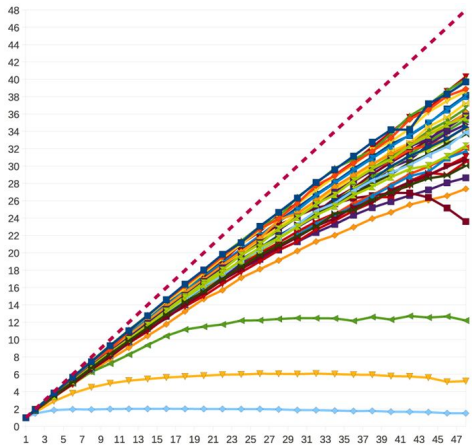

図１ slim モデル検査器による並列状態空間構築のスケーラビリティ（34 例題，48 コアマシン，横軸：コア数，縦軸：速度向上比）

(3) モデル検査向けのグラフ同型性判定技法

グラフ書換えに基づくモデル検査の状態管理では，多数のグラフ間の同型性判定が重要な役割を演ずる．これを効率的に行うには，グラフの形を一意的に表現するグラフ正規形を用いることが有効だが，正規化の手間が問題となる．そこで，少しずつ異なる多数のグラフに対して，グラフ間の差分情報に着目してグラフ正規化の全体コストを削減する手法を開発して，試験実装と評価を行った．提案アルゴリズムは彩色単純グラフにおけるグラフ正規化に用いられる McKay のグラフ正規化アルゴリズムをグラフ書換え系向けに最適化することで実現し，バブルソートモデルにおいてグラフ１個当たり節点数によらない手間でグラフ正規化を実現することを証明した．

(4) 統合可視化環境の整備と公開

高水準モデリング言語を有用なツールとするためには，モデル検査によってバグの有無の検証を可能にするだけでなく，バグの有無にかかわらずモデルの性質や挙動の理解を助ける機能が重要となる．そこで，(1)(2)の諸機能に加えて，状態空間の可視化機能をもつ統合環境 LaViT（図２）およびグラフ書換え過程の可視化を行う Graphene の整備を進めて公開した．あわせて，LMNtal コンパイラと実行系 slim も新たに github からオープンソースソフトウェアとして公開した．

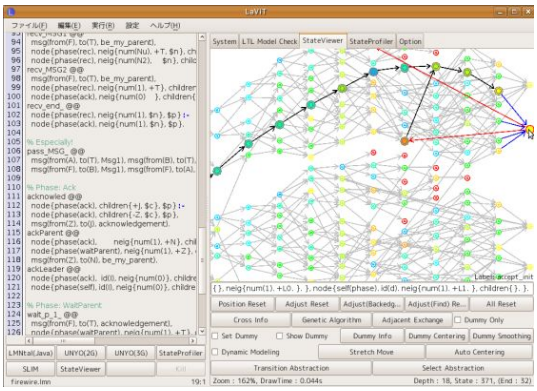

図２ LMNtal 統合開発環境 LaViT 上での Firewire プロトコルの検証可視化

(5) HydLa 記号実行シミュレータ Hyrose の実装

制約概念に基づくハイブリッドシステムモデリング言語 HydLa は，不確定性をもつシステムの表現とシミュレーションの枠組の提供を最大の特徴とする．本研究では，開始時点で提案されていた非決定実行アルゴリズムに対し，実装を念頭に置いた詳細化を行った．変数とは別に記号定数の概念を導入して記号実行アルゴリズムを定式化し，数式処理エンジンをバックエンドとする Hyrose 上に実現してその妥当性を確認した．これによって，初期条件の一部が区間値として与えられたシステムや記号パラメタをもつシステムの記号実行に基づくシミュレーションが可能になった．このようなシステムは一般に複数の定性的に異なる軌道をもつが，Hyrose は初期値に関する場合分けを行ってその全解を出力することができる．

制約に基づくハイブリッドシステム記述言語の実装事例はきわめて少なく，本研究では多くの観点から細部の仕様と実装を詰める必要があった．妥当な処理系とするには以下の点で従前のアルゴリズムの詳細化を行う必要性が新たに判明し，それぞれに対して設計と実装を行った．

① モデルが暗黙のうちに仮定する軌道の連続性の補完方法
② シミュレーション開始時刻における左極限値の扱いの確定
③ 微分方程式を含む制約の無矛盾性判定
④ 不確定性をもつシステムにおける離散変化時刻の計算

(6) HydLa からハイブリッドオートマトンへの変換

Hyrose の無限時間モデル検査器への発展を目指して，HydLa モデルの抽象解釈に基づく状態空間構築手法に基づいたハイブリッドオートマトン変換アルゴリズムを設計し実装した．提案する HydLa の抽象実行アルゴリズムは，パラメタを用いて抽象化された HydLa プログラムの到達可能範囲（reachable set）の不動点を求めるアルゴリズムである．本アルゴリズムにより求められた到達可能範囲は

対象のハイブリッドシステムの全状態を漏れなく表現しているため，ハイブリッドオートマトンとして出力可能である．そのため本アルゴリズムは HydLa のハイブリッドオートマトンへの変換アルゴリズムとして用いることができる．さらに，得られたオートマトンを活用することで，HydLa モデルのシミュレーションの高速化も図ることができることを示した．

(7) 制約プログラミングの特性を活かした Hyrose 処理系の最適化

Hyrose の実行アルゴリズムは，軌道を決定する無矛盾極大制約集合の探索や次の離散変化時刻の決定を含めて，制約充足問題の求解を基本演算として多数回実行する．この制約求解に対して，求解結果の再利用や制約間の依存関係解析に基づく最適化アルゴリズムを開発し実装を行った．また，この最適化が軌道求解の計算量を改善することを実際の処理系の上で確認し，処理系のスケーラビリティの大幅向上に対する見通しを得た．

(8) Hyrose への対話実行機能の導入

制約プログラムの実行が期待通りに進まない場合，挙動の理解や解析を支援する機能が重要となる．特に制約集合が予想に反して充足不可能であった場合にその理由を解析するために，極小矛盾集合を求めて提示する機能を対話実行系に組み込んだ．

(9) 例題記述に基づく Hyrose の問題表現・求解能力の確認

パラメタを含む多くの例題の記述とその非決定実行を通じて，HydLa および Hyrose の能力の確認を行った．たとえば ①複数のパラメタをもつ熱気球モデルに対して気球が落下しないための初期条件を求める問題，②倒立振子が倒れないための制御条件を求める問題（図３），③溝のある地面を跳ねる質点が目標地点に到達するための初期条件を 50 通りの定性的に異なる軌道の場合分けから求める問題，④TCP の輻輳制御アルゴリズムのシミュレーション，⑤質点の同時多重衝突によって制約が充足不可能になるモデルに対し，初期条件に摂動を加えることで特異点を回避して解析を行う例，などを記述し実行した．

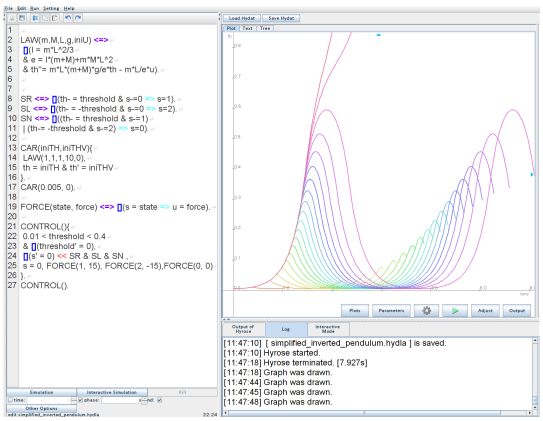

図３ HydLa 統合開発環境 HIDE による倒立振子制御問題の記述とシミュレーション

〔研究の特色と位置づけ〕

本研究は，プログラミング言語とシステム検証の境界領域において，通常のプログラム実行と検証とを統合する実用的な高水準言語処理系を構築する点を最大の特徴とする．

研究のベースとなる言語モデルはいずれも本研究グループが創出した高いオリジナリティをもつ枠組である．LMNtal は Maude をはじめとする既存の書換え型高水準モデリング言語と比べて少ない記述量を特徴とする．モデル検査機能をもつグラフ書換え系としては Groove が知られるが，LMNtal はラムダ計算，CHR，BRS を含む多様な計算モデルと関連付けがなされている点で統合モデルとしての役割を果たしている．HydLa は，ハイブリッドオートマトンを理論的基礎とする他の大多数の高水準ハイブリッド言語と異なり，データ構造のみならず制御構造にまで一貫して制約概念を採用している点を最大の特徴とする．

また，LMNtal は記述対象のもつ対称性（に起因する状態空間爆発）への自動対処機能，HydLa は結果の正当性や精度の保証された高信頼実装技術が，検証分野への展開において独自の利点を与えると期待できる．単なるモデル検査にとどまらず，どちらの言語処理系も対象系の分析と理解を支援していることも特徴で，従来の低水準言語を用いた大規模検証とは相補的な役割を演じる．

〔波及効果〕

本研究は，プログラミング言語，システム検証，並列処理，精度保証数値計算といった情報科学の多くの分野の相互交流を促進することを意図して実施し，上記の各分野の研究者との研究交流を行いながら進めてきた．成果である高水準モデリング言語処理系はこれまで多くの国際会議や海外セミナー等でデモ付きで紹介し，過去に交流のなかった研究者からも関心を集めるに至っている．

モデリング言語は，計算生物学やロボティクス，制御工学などを含む広範な関連領域をもち，強力なモデリング・検証ツールの確立と普及は，情報科学にとどまらず工学全体への学際的波及効果が期待できる．サイバーフィジカルシステムと大規模システムの検証技術は，それぞれ情報科学におけるグランドチャレンジとなりうる重要分野である．その確立にはさらに多くの蓄積が必要となるが，本研究は，グラフや集合，方程式・不等式など，情報科学の枠にとどまらない一般的概念に基づく高水準モデリング言語の可能性を具体的に提示した点が大きな意義であると考える．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１１件）

(1) 安田竜，吉田健人，上田和紀： LMNtal 並列モデル検査における状態生成数削減及び高速化， 人工知能学会論文誌，Vol.29，No.1 (2014)，pp.182-187．(査読有)
DOI: 10.1527/tjsai.29.182

(2) 松本翔太，上田和紀： ハイブリッド制約言語 HydLa の記号実行シミュレータ Hyrose， コンピュータソフトウェア，Vol.30，No.4 (2013)，pp.18-35．(査読有)
DOI: 10.11309/jssst.30.4_18

(3) Cyrille Artho, Masami Hagiya, Richard Potter, Yoshinori Tanabe, Franz Weitl, Mitsuharu Yamamoto: Software model checking for distributed systems with selector-based, non-blocking communication. ASE 2013: 169-179.(査読有)
DOI: 10.1109/ASE.2013.6693077

(4) 前岡 淳，田辺 良則，石川 冬樹： Java PathFinderにおける探索打ち切りポリシーを用いたヒューリスティック探索．コンピュータ・ソフトウェア 30(3)，pp.109-122，2013．(査読有)
DOI: 10.11309/jssst.30.3_109

(5) D. Ishii, A. Goldsztejn, and C. Jermann. Interval-based projection method for under-constrained numerical systems. Constraints Journal, 17(4):432-460, 2012．(査読有)
DOI: 10.1007/s10601-012-9126-y

(6) K. Ueda, S. Matsumoto, A. Takeguchi, H. Hosobe, and D. Ishii. HydLa : A High-Level Language for Hybrid Systems. In Logics for System Analysis Workshop (LfSA), pages 3-17, 2012．(査読有)
http://www.ls.cs.cmu.edu/LfSA12/LfSA12.pdf

(7) Kazunori Ueda and Seiji Ogawa: HyperLMNtal: An Extension of a Hierarchical Graph Rewriting Model. Künstliche Intelligenz, Vol.26, No.1 (2012), pp.27-36．(査読有)
DOI: 10.1007/s13218-011-0162-3.

(8) D. Ishii, K. Ueda, and H. Hosobe. An interval-based SAT modulo ODE solver for model checking nonlinear hybrid systems. International Journal on Software Tools for Technology Transfer (STTT), 13(5):449-461, 2011．(査読有)
DOI: 10.1007/s10009-011-0193-y

(9) 後町将人，堀泰祐，上田和紀： LMNtal 実行時処理系の並列モデル検査器への発展，コンピュータソフトウェア, Vol.28，No.4 (2011)，pp.137-157．(査読有)
DOI: 10.11309/jssst.28.4_137

(10) Watcharin Leungwattanakit, Cyrille Artho, Masami Hagiya, Yoshinori Tanabe, Mitsuharu Yamamoto: Model checking distributed systems by combining caching and process checkpointing. ASE 2011: 103-112．(査読有)
DOI: 10.1109/ASE.2011.6100043

(11) 渋谷俊，高田賢士郎，細部博史，上田和紀： ハイブリッドシステムモデリング言語 HydLa 処理系の実行アルゴリズム，コンピュータソフトウェア，Vol.28，No.3 (2011)，pp. 167-172．(査読有)
DOI: 10.11309/jssst.28.3_167

〔学会発表〕（計１８件）

(1) Kazunori Ueda, A Hybrid Constraint Language HydLa and Its Implementation. Halmstad Colloquium, Halmstad University, Sweden, 2014-03-11. (invited lecture)

(2) Alimujiang Yasen, 上田和紀： Encoding type systems into HyperLMNtal，日本ソフトウェア科学会第 30 回大会 (JSSST2013)，萌芽 3-1，2013-09-11

(3) 松本翔太，上田和紀： ハイブリッドシステム制約言語 HydLa の数式処理実行系へのアフィン演算の導入，日本ソフトウェア科学会第 30 回大会(JSSST2013)，一般 3-1，2013-09-12

(4) 宮原和大，上田和紀：グラフ書換え系におけるグラフ構造の効率的な一意バイト列生成手法，日本ソフトウェア科学会第 30 回大会(JSSST2013)，PPL4-3，2013-09-13

(5) 信夫裕貴，田辺良則，上田和紀： LMNtal におけるグラフ書換え操作の Coq による形式化，日本ソフトウェア科学会第 30 回大会(JSSST2013)，PPL5-2，2013-09-13.

(6) Yuuki Shinobu, Yoshinori Tanabe, Kazunori Ueda: Formalization of the Graph Rewriting Operations of LMNtal by Coq, 11th Asian Symposium on Programming Languages and Systems (APLAS 2013), 2013-12-10.

(7) Kazuhiro Miyahara and Kazunori Ueda: Optimized Canonical Graph Labeling

Algorithm for Graph Rewriting Systems, 11th Asian Symposium on Programming Languages and Systems (APLAS 2013), 2013-12-10.

(8) 和田亮, 松本翔太, 上田和紀: ハイブリッド制約言語 HydLa の対話的な実行方式の実装, 第 11 回 ディペンダブルシステムワークショップ (DSW 2013), 2013-12-26

(9) 河野 文彦, 松本 翔太, 上田 和紀: 制約の静的解析を用いた HydLa 処理系の最適化, 2013 年度人工知能学会全国大会論文集, 2J1-1, 2013-06-05

(10) 目黒 学, 宮原 和大, 上田 和紀: LMNtal による Bigraph のエンコードおよびモデル検査の実現, 第 10 回 ディペンダブルシステムワークショップ (DSW 2012), 神戸, https://sites.google.com/site/jssstdsw/dsw2012 (14 pages) 2012-12-11

(11) 竹口 輝, 和田 亮, 松本 翔太, 細部 博史, 上田 和紀: ハイブリッド制約言語プログラムのハイブリッドオートマトンへの変換アルゴリズム, 日本ソフトウェア科学会第 29 回大会論文集 2A-3 (10 pages), 東京, 2012-08-22

(12) 松本 翔太, 上田 和紀: ハイブリッド制約言語 HydLa の記号実行シミュレータ Hyrose, 日本ソフトウェア科学会第 29 回大会論文集 5C-4 (16 pages), 東京, 2012-08-24

(13) 目黒 学, 谷口 直輝, 上田 和紀: 複数の計算モデルをサポートするモデル検査器の実現, 日本ソフトウェア科学会第 29 回大会論文集, 6A-4 (13 pages), 東京, 2012-08-24

(14) Shota Matsumoto, Akira Takeguchi, Kazunori Ueda and Hiroshi Hosobe: Hybrid Constraint Language HydLa and Its Implementation. The 15th International Conference on Hybrid Systems: Computation and Control (HSCC 2012), Beijing, (Poster), 2012-04-17

(15) 竹口輝, 松本翔太, 上田和紀: ハイブリッドシステムモデリング言語 HydLa を用いたシステム解析, ディペンダブルシステムワークショップ&シンポジウム (DSW & DSS 2011)論文集, 京都, 2011-12-14

(16) 清水涼子, 川端聡基, 上田和紀: Explicit-time method によるモデル検査器 SLIM におけるリアルタイムモデル検査, 日本ソフトウェア科学会大会第 28 回大会論文集, 4C-3, 那覇, 2011-09-28

(17) 田辺 良則, Cyriile Artho, Watcharin Leungwattanakit, 山本 光晴, 萩谷 昌己: ネットワークアプリケーションのマスター・スレーブ方式モデル検査アルゴリズムについて. 日本ソフトウェア科学会大会第 28 回大会, 5B-3, 那覇, 2011-09-29

(18) 小川誠司, 目黒学, 上田和紀: 階層グラフ書換えモデルを拡張した HyperLMNtal の実現, 2011 年度人工知能学会全国大会 (第 25 回) 論文集, 2I1-4, 盛岡, 2011-06-01

〔図書〕(計 1 件)

(1) Kazunori Ueda: Towards a Substrate Framework of Computation. To appear in Concurrent Objects and Beyond (COB 2012), LNCS 8665, Springer-Verlag, 2014, 26 pages.

〔その他〕

ホームページ等

(1) http://www.ueda.info.waseda.ac.jp/lmntal/

(2) http://www.ueda.info.waseda.ac.jp/hydla/

６．研究組織

(1)研究代表者

上田 和紀 (UEDA, Kazunori)
早稲田大学・理工学術院・教授
研究者番号：10257206

(2)研究分担者

田辺 良則 (TANABE, Yoshinori)
国立情報学研究所・アーキテクチャ科学研究系・教授
研究者番号：60443199

(3)連携研究者

細部 博史 (HOSOBE, Hiroshi)
法政大学・情報科学部・教授
研究者番号：60321577

石井 大輔 (ISHII, Daisuke)
東京工業大学・情報理工学研究科・助教
研究者番号：00454025