様式 C-19

科学研究費補助金研究成果報告書

平成２２年５月１２日現在

研究種目：基盤研究(C)
研究期間：2007～2009
課題番号：19500026
研究課題名（和文）　コレオグラフィ記述に基づく組込みシステムの高信頼性設計技法

研究課題名（英文）　A reliable design method for embedded systems based on choreography descriptions

研究代表者
結縁　祥治　（YUEN, Shoji）
名古屋大学・大学院情報科学研究科・教授
研究者番号：70230612

研究成果の概要（和文）：
集中的な制御を仮定しない分散並行実行の概念としてのコレオグラフィーに基づいたシステム記述とその設計技法を示した。具体的には、家電ネットワークの優先度を導入した記述およびユーザインタフェースの設計技法を提案し、さらに、時間オートマトンを組み合わせた動作モデルを提案し、状態の順序にループのない場合には分散記述と大域記述が同じ能力を持つことを示した。このことは割込みの動作検証が基本的に時間オートマトンで可能なことを示す。

研究成果の概要（英文）：
We investigated a design method based on the notion of 'choreography' which controls a distributed concurrent system without any central control mechanism. We have shown a distributed construction from a global description with priority in the home appliance network and GUI application software. We also investigated a composition of timed automata, called 'Control automaton', with a global transition where we showed that the expressive power remain unchanged if there is an order between states. By this, it is shown that a timed automaton is used to verify the timed behavior with interrupts.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,000,000	300,000	1,300,000
2008 年度	700,000	210,000	910,000
2009 年度	1,400,000	420,000	1,820,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：プログラム言語、並行プログラミング

１．研究開始当初の背景

組み込みシステムの規模の増大に伴って組み込みシステムは分散システムとなっている。分散システムにおいて実行効率をあげ、応答性を向上させるためにシステムの構成要素であるコンポーネントは並行に実行されるのが一般的である。

並行プログラムは、逐次的プログラムに比

べてシステム全体の状態が同定しにくい。並行プログラムでは、通常、動作することのできる制御フローが複数存在し、どのタイミングでどの制御フローが実行されるのか一意に定まらない。設計の段階でこの予測に洩れがあったり、複数の外部イベントが複合的に影響して予想外の振舞いをすることにより、システムとして設計にない状態に陥る場合がある。このような状態はシステムに致命的な障害をもたらすことが多く、並行システムの信頼性を低下させる結果となる。

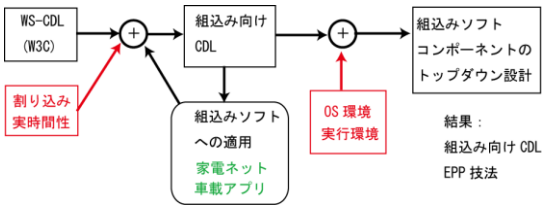
高信頼の組込みソフトウェアを構成するためには、並行分散計算を自然に記述する枠組みを用意する必要がある。この枠組み上で振舞いの性質を検証することができれば、並行分散組込みシステムの信頼性向上に大きく貢献すると期待される。

２．研究の目的

本研究では、コンポーネントが疎結合されて構成される組込ソフトウェアにおいて、全域的な記述からそれぞれのコンポーネントに配置すべきプログラムを導出する設計技法を提案する。コレオグラフィ記述言語 (Choreography Description Language, 以下、CDL) を用いて全体状態を記述し、通信プロセスモデルの理論である π 計算理論に基づいて、コンポーネントの分散配置を行う新たなトップダウンの設計手法を提案する。この技法によって、組込みシステムの設計を効率的に行い、動作の信頼性を向上させることが目的である。

３．研究の方法

CDL 記述は、通信に注目したサービス指向アーキテクチャ(SOA) の記述に適している。組込みシステムにおいてもSOA 技術が導入されつつある。本研究では、この点に着目して、組込みソフトウェアに応用する。組込みシステムは目的や要求される性質が多岐にわたるため、具体的な問題でCDL 記述し、CDL 記述にどのような機能が必要かを検討する。その後、一般的なアプリケーションの構築技術について検討を進めた。研究全体のシナリオを以下の図に示す。



WS-CDL にもとづいて以下の適用事例を通じて、組込みシステムの動作に必要な割り込みや実時間性の記述を加え、組込み向けの拡張を議論した。さらに、実行環境を定義することで、その実行環境に対するEPP の具体的な手法を導出し、トップダウンの設計手法を示す。実行環境もできるだけ柔軟に定義できるような枠組を提案する。研究の結果として、組込み向けCDL の提案と、EPP の適用条件および適用できる場合の具体的な手法を示す。

４．研究成果

本課題では以下の３項目について研究を行い成果を得た。

(1) 家電ネットワークにおけるコレオグラフィー記述

家電製品はネットワークで接続され、連携しながら動作する。家電ネットワークは、各機器が信号を関連する機器から受信することと、関連する機器に発信することによって全体として統合された動作を実現する。全体を集中的に管理する機器は存在せず、それぞれ自分の機能のみで通信を行う。このような状況は、コレオグラフィーによる並行動作で自然にモデル化でき、EPP の手法を用いることによって、全体の統合された振舞いから各機器の振舞いを導出することができる。

このようなネットワークの振舞いにおいて問題となるのは、個々の機能から全体の振舞いを構成する際に競合が発生することである。個々の機器が各自の振舞いに従って動作する際に、タイミングによってランプのON/OFF のように相反する動作が可能になる場合がある。全体を制御する機器が存在しない場合、このような競合を制御するのは難しいため、本研究では、優先度を導入することで競合を解消する拡張を行った。統合した振舞を記述した全体的な優先度を個々の機器が受ける信号間の局所的な優先度で解決することができる体系を提案し、優先度つきEPP の実現のプロトタイプを実装した。

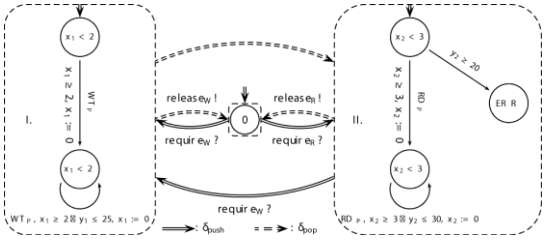
(2) GUI コンポーネントの振舞いに対するコレフォグラフィー記述

本研究では，GUI アプリケーションに対して，その振る舞いをユーザ・内部システム・GUI コンポーネントの間の通信系列で特徴化し，通信指向プログラミング手法を適用する．通信指向プログラミングでは，2 者間の通信の系列をシステム全体の振る舞いとして大域的に記述し，この大域記述を通信の参加者ごとに独立したプロセスに分解する．このためにGUI アプリケーションの大域的な記述としてGUI-CDL，局所的な記述としてGUI-π を定義し，GUI-CDL からGUI-π への変換GUI-EPP を定義する．GUI アプリケーションでは，ユーザとの通信は必要に応じて制限される．この特徴を通信における可視性として導入して，高信頼のGUI プログラミングを実現した．

この手法に基づいてOcamlを用いてGUIアプリケーションを構築するプロトタイプを作成し、GUIπからOcamlへの変換が自然に可能であり、コレオグラフィーに基づいたGUI応用プログラムに対するトップダウンの設計手法：GUI-CDL⇒GUI-π⇒Ocamlを具体的に示した。

(3) 制御オートマトン

時間オートマトンの集合に対して、大域的なシンボルによって振舞を切り替えるモデルを提案した。(図)



これは、組込みシステムのタスクがスケジューラによって切り替わることをモデル化する。さらに、切替えを外部イベントとみなすことによって割込みハンドらによるシステムの振舞を正確にモデル化する。時間オートマトンでモデル化することによって、タスクがスリープしている間も時間が経過することをモデル内で表現することができ、タスクが割込みやスケジュールの不具合によって動作しなくなる状況を検出できるようになった。一般には、再帰的な大域ループが存在する場合には、制御オートマトンにおける到達可能性は決定不能である。しかし、割込みの優先度に対応する状態間の順序を導入すると、等価な単一の時間オートマトンに変換することができ、到達可能性が計算可能になることを示した。このことにより、厳密な順序を割込みハンドラに対してつけた場合には、システムの振舞を検査するアルゴリズムが存在することを示すことができた。これは、時間に関する大域的な情報を単一のタスクの振舞いに変換することによる基本的な検証手法が存在することを示している。

(4) 研究成果の位置づけ

本課題は、全体の状態を把握するプロセスが存在しないコレオグラフィーに基づいた通信指向プログラミングによるシステム構築の具体例から、通信指向プログラミングを組込みシステムに応用するための手法を提案することが目的であった。この点において、優先度、時間、通信隠ぺい機構の３項目について研究を行った。優先度については、家電ネットワークの事例について通信指向プログラミングが応用できることが示された。しかし、優先度を導入した計算体系および EPP の一般的な体系の提案は、本研究の期間内ではできていない。優先度は、組込みシステムにおける基本的な振舞の概念であり、実時間性が要求される組込みシステムは必要な拡張であるため、さらに研究と続ける必要がある。

時間の概念については、時間オートマトンをベースにしたモデルを拡張した。しかし、通信指向プログラミングへの応用にはギャップがある。

GUI 応用プログラミングでは、通信の隠ぺい機構を導入することで、具体的なトップダウン的な基本設計手法を提案することができた。しかし、計算体系については、さらに単純化して検証を容易にすることができると予想されるので、理論的な研究を継続する必要がある。

(5) 今後の展望

本課題では、具体的な事例について通信プログラミングを適用することを主眼において研究を進めたため、理論的な体系を整備することが望まれる。既存の優先度、時間が導入された通信プロセス計算の体系から、通信指向向けの拡張されたコレオグラフィーを導出することが本課題の結果から得られた今後の課題である。

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４件）

1. 横山 哲郎, 今井 敬吾, 曾 剛, 冨山 宏之, 高田 広章, 結縁 祥治, `動的電圧制御システムにおける評価戦略選択に基づく高効率消費エネルギー関数型プログラミング,' 情報処理学会論文誌, vol.2, no.2(PRO 41), pp.54-69, March 2009.査読有
2. Irek Ulidowski and Shoji Yuen, `Generating Priority Rewrite Systems for Osos Process Langauges, ' Information and Computation, vol.207, no.2, pp.120-145, February 2009.査読有
3. 結縁祥治, `通信プロセス計算とその時間拡張,' システム制御情報学会誌, vol.52, no.9, pp.322-327, September 2008.査読有
4. 末次 亮, 結縁 祥治, 阿草 清滋, `通信プロセスモデルによる AIBO OPEN-R プログラムのデッドロックフリー解析手法,' 情報処理学会論文誌, vol.48, no.9, pp.2915-2924, September 2007.査読有

〔学会発表〕（計 15 件）

1. Keigo Imai, Shoji Yuen, and Kiyoshi Agusa, `Session Type Inference in Haskell,' In PLACES'10: Programming Language Approaches to Concurrency and Communication-cEntric Software, pp.43-52, March 2010. 査読有, Paphos(キプロス)
2. 今井敬吾、結縁祥治、阿草清滋. ″極性を持たないセッション型システム″, 第12回プログラミングおよびプログラミング言語ワークショップ(PPL2010), pp.16-30, 2010、査読有、高松(香川)
3. 下村 翔, 結縁 祥治, `コレオグラフィに基づく高信頼通信指向 GUI プログラミング,' 電子情報通信学会技術研究報告, March 2010. 査読無、鹿児島大学(鹿児島)
4. 坂野 吉隆, 結縁 祥治, `計算資源へのアクセス能力に基づく競合検査とデッドロック検査のための型解析,' 電子情報通信学会技術研究報告, March 2010. 査読無、鹿児島大学(鹿児島)
5. 水野 洋樹, 結縁 祥治, `実行履歴にもとづくマルチコア実時間応用プログラムのデバッグモデル,' 電子情報通信学会技術研究報告, vol.109, no.343, pp.49-54, December 2009.査読無、香川大学(高松)
6. Guoqiang Li, Shoji Yuen, and Masakazu Adachi, `Environmental Simulation of Real-Time Systems with Nested Interrupts,' In Theoretical Aspects of Software Engineering (TASE2009), pp.21-28, July 2009. 査読有、天津(中国)
7. 伴 潤, 今井 敬吾, 結縁 祥治, `Maudeによる否定を含んだ構造操作意味定義インタプリタと等価性検証器の構築,' 電子情報通信学会技術研究報告, vol.109, no.40, pp.49-54, May 2009. 査読無、秋田大学
8. Keigo Imai, Shoji Yuen, and Kiyoshi Agusa, `A Full Implementation of Session Types,' In 第11回プログラミングおよびプログラミング言語ワークショップ(PPL2009), p.44-56, March 2009. 査読有、 高山(岐阜)
9. Li Guoqiang, 結縁祥治, 足立正和, `Environmental Simulation of Real-Time Systems with Nested Interrupts by Maude,' 第11回プログラミングおよびプログラミング言語ワークショップ(PPL2009), pp.133-147, March 2009. 査読有、高山(岐阜)
10. 馬場 敬, 結縁 祥治, 阿草 清滋, `Apache Cocoon Flowscript のモデル検査による Web 応用プログラムの動作検証,' 電子情報通信学会技術研究報告, vol.108, no.444, pp.017-022, March 2009. 査読無、(電子情報通信学会ソフトウェアサイエンス研究会,佐賀大学 2009/03/02-03)
11. 足立正和, 末次亮, 結縁祥治, 手嶋茂晴, 佐野範佳, `充足可能性判定に基づくリアルタイムシステムのスケジューリング解析,' 組込みシステムシンポジウム 2008, pp.41-49, 査読有、October 2008. 東京
12. バンダリ さくら, 結縁 祥治, 阿草 清滋 , `Communication Centered Programming of Integrated Services with Priority in Home Appliance Network,' Apsec 2007, Workshop on Service Oriented Architecture, 査読有、2007. 名古屋
13. Ryo Suetsugu, Shoji Yuen, and Kiyoshi Agusa, `A Synchronization Flow Analysis of Concurrent Objects in Aibo Open-R Programs Based on Communicating Processes,' In 14th Asia-Pacific Software Engineering Conference, pp.366-373, 査読有、2007. 名古屋
14. バンダリ さくら, 結縁 祥治, 阿草 清滋, `分散環境における家電機器の連携動作の記述手法,' 第５回ディペンダブルシステムワークショップ DSW2007, no.No,48, pp.35-44, 査読無、July 2007. 函館
15. 今井敬吾、結縁祥治、阿草清滋.″セッション型に基づく高信頼性ネットワークプログラムのHaskell言語による実装″,第５回ディペンダブルシステムワークショップ DSW2007, no.No,48, pp.95-106, 査読無、July 2007. 函館

〔図書〕(計０件)
〔産業財産権〕
○出願状況 (計０件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況 (計０件)

名称：
発明者：
権利者：

種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
結縁祥治（YUEN, Shoji）
名古屋大学・大学院情報科学研究科・
教授
研究者番号：70230612

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：

(4) 研究協力者
李　国強（LI, Guoqiang）
今井敬吾（IMAI, Keigo）