博士論文

モデル検査を用いた心拍モニタリングに基づく車体制御システムの高信頼化

2021 年 3 月

井川　直

岡山県立大学大学院

情報系工学研究科

目次

第 1 章

まえがき

近年，人工知能 (AI) の技術の発展によって車の自動運転技術の開発が盛んに行われている．自動運転下では車内環境や外部環境の情報に基づき，ドライバが運転に介入することなく車速や車線維持のための操作が適切に制御される．自動運転は完全自動化を目的として，自動運転レベルが SAE インターナショナル (Society of Automotive Engineers, 米国自動車技術者協会) によって定義されている [1]．現在において自動運転レベル 2 に位置付けられる自動運転車が実用化されており，速度の加減速やステアリング操作の部分的な運転の自動化が実現している．自動運転レベル 2 の段階では，運転の主体はドライバであるため部分的な運転の自動化はシステムによるドライバの運転支援を目的としている．ADAS (Advanced Driver-Assistance Systems, 先進運転支援システム) [2] は代表的な運転支援システムであり，ACC (Adaptive Cruise Control System, 車間距離制御) や LKAS (Lane Keeping Assist System, 車線逸脱防止支援システム) などの機能から構成される．

このような部分的な運転の自動化が進展する中で，ドライバの体調に基づく運転支援が注目されている．ドライバの不調を検知した場合に警告を発して注意を促したり，自動運転へ切り替えたりすることで交通事故やそれによる 2 次被害を防止することが可能となる．一例としてドライバの居眠り防止が挙げられる．ドライバの眠気の検出は，車の挙動や表情，目の動きなどを元に画像処理と機械学習によって行う手法が提案されているが，心拍などの生体情報が，眠気の検出にはより適していると考えられている [3]．心拍は眠気が表情や目に影響を及ぼす前に変化するため，眠気の早期検出に役立てることができる．また，心拍は眠気だけでなく不整脈をもたらす心疾患の検出にも利用できる．そこで本研究では，ドライバの心拍モニタリングに基づく運転支援に着目した．

ドライバの心拍モニタリングには，心電計 (Electrocardiograph : ECG) [4] や脈波計

[5] が使用されてきたが，既存の心拍モニタリング機器のほとんどは直接皮膚に接触するタイプのインタフェースであるため不快感やアレルギーなどによりユーザに掛かる負担が大きい．そのため，非接触で心拍モニタリングを実現するシステムが強く望まれている．しかし，非接触による心拍モニタリングは車の揺れやユーザの体動などの外乱の影響を強く受けるため運転中に高精度の計測を行うことは困難である．また，心拍モニタリングに基づく制御の実現には高いリアルタイム性が要求されるため，求められる時間制約を満たした上で制御が実行されるように高い信頼性も確保する必要がある．リアルタイム性をもつ心拍モニタリングシステムの品質保証も重要な課題である．

本研究では，高精度な心拍モニタリングに基づく高信頼な車体制御システムを実現する．まず，車載環境での非接触センサによる心拍モニタリングの高精度化を実現するため，心電波形の形状に着目したフィルタリングに基づいて心拍計測を行う手法を提案する．さらに，モニタリングに基づく車体制御の高信頼化を実現するため，運転制御構造をモデル化した実時間システムを対象に，モデル検査を用いて複雑なリアルタイム制御の妥当性検証を自動的に行うための手法を提案する．

前者の非接触センサによる心拍モニタリングの高精度化ついては，UWB センサを用いた非接触による高精度な心拍間隔の計測について述べる．

非接触の心拍モニタリングシステムとしては，Capacitive coupled ECG [6] を使ったシステムや連続波ドップラレーダ [7] を使ったシステムが開発されてきた．特に近年では Ultra Wide Band (UWB) センサを使って心拍や呼吸などの生体情報を検出する研究が数多く行われている [8, 9, 10, 11]．UWB は非常に広い周波数帯を利用する無線通信であり，近距離で使用することで高精度なセンシングを可能とする．これらの研究では，検出の高精度化や複数対象からの同時検出などが提案されており，UWB センサに対する期待が高いことが伺える．

[8, 9] では既存の復調技術である Complex Siganl Demodulation (CSD) と Arctangent Demodulation (AD) を組み合わせることで呼吸と心拍の混合信号から高精度に各信号を分離し，複数人の呼吸・心拍を同時検出を提案している．ほかにも，信号を分解する手法としてアンサンブル経験的モード分解 (Ensemble Empirical Mode Decomposition : EEMD) を用いることで効率的に呼吸と心拍を分解する手法 [10] やレーダから得られた信号のピークのパターンに着目して心拍間隔を高精度に検出するトポロジー法と呼ばれる手法が提案されている [11]．上記の他にもレーダを用いた心拍や呼吸の様々な検出手法が提案されている [12]．また，特定の状況を想定して生体情報を検出する手法も提案されている．例として，動く人体を正確に追跡することで非接触で心拍検出を実現する手法 [13] や車の車内など，対象の近くに反射物が多く存在し，受信した生体情報の信号が反射物か

らの信号によって弱くなる環境下で生体情報を取得する手法をシミュレーションによって示している研究 [14] がある．以上のように UWB センサを用いて非接触で呼吸や心拍といった生体情報を検出しようとする研究では，この数年で多様な手法が提案されている．

一方，MIMO (Multi Input Multi Output) [15] レーダを用いた非接触心拍モニタリングについても研究がなされている．レーダは送信波と反射波の差分によって対象までの距離や方向を求めることが可能なため物体検出に用いられ，ミリ波や MIMO 技術などが採用される．その研究トピックとしては，単一の物体だけでなく複数の物体の検出や検出した物体の位置情報を 2 次元および 3 次元空間上にマッピングする 2 D (3 D) マッピング，人の行動識別など様々な応用が研究されている [16]．また，民間に普及しつつある IEEE 802.ad 規格に基づくミリ波機器による物体検出を評価し，レーダを使った物体検出の低コスト化を検討している研究も存在する [17]．さらに，MIMO レーダを用いて胸の動きや心臓の拍動などの mm オーダの微細な運動を捉えることで呼吸や心拍を非接触で検出する試みもなされている．[18] は，寝返り等でアンテナとの相対位置が変化する睡眠時における心拍の高精度推定を提案している．[19] では心拍と呼吸の同時検出手法が提案されており，1 m の距離から椅子に座った状態の被験者を対象に，座った状態から体を前後に揺らすなどの動きを加えた状況であっても平均して 96 % の精度で心拍を検出している．心拍数の正解データとしてパルスオキシメータを被験者の指先に装着している．

これまでに著者らは，UWB センサを用いて非接触で心拍を計測するシステムを開発してきた [20, 21]．UWB センサは，極短いパルス波を用いるインパルス方式によってセンシングを行う．このシステムでは UWB センサから得られたデータに対してノイズフィルタリングを施すことによって，データから心拍を計測することを可能としている．また，本システムを運転中のドライバに対して適用し，運転中の車内で発生する体動や外乱からのノイズをノイズフィルタリングによって取り除くことで，心拍を計測できることを示している [21]．さらに，計測された心拍データをもとに心拍間隔を算出することで精神状態を推定するための重要な生体情報を取得できる見通しを得ている [20]．しかし，実際に運転中の車内で計測した心拍データをもとにして心拍間隔を算出した上で，その数値を MIMO レーダなどの既存の技術と比較して，定量的に評価するまでには至っていない．

本論文ではこれらの成果に基づいて，車内で計測という状況を想定した場合にも，UWB センサを用いた非接触での心拍計測によって心拍間隔が正しく算出できることを示す．本システムの有効性を評価するために，実際に運転中の車内において適用実験を実施した．従来，非接触での動体検知にはミリ波レーダが広く用いられてきたことから，本論文ではミリ波レーダによる計測を同じ条件にて実施した上で，その精度を比較している．ここで，心拍間隔の正解データとしては従来の接触型心拍モニタリング機器によって計測され

たデータを用いている．精度の評価は異なる手法間の一致度をグラフを使って視覚的に表示可能である Bland-Altman プロット [22] を用いており，既存の心拍モニタリング機器から得られた心拍間隔データを基準として，UWB センサおよびミリ波レーダで得られた心拍間隔をそれぞれプロットすることで，どちらの一致度が高いかを評価している．併せて，心拍間隔を元に算出されるストレス指標 LF/HF [23] を用いて，UWB センサと心拍モニタリング機器それぞれから得られる LF/HF の誤差が十分小さいことを示すことで UWB センサによる心拍間隔計測の有用性を示す．

後者の車体制御の高信頼化については，実時間システムのモデルの 1 つである時間ペトリネット (Time Petri Nets：TPN) によってモデル化された運転制御機構を対象として，モデル検査手法を用いて妥当性検証を行うための手法を開発する．有界モデル検査を用いた実時間システムの検証について述べる．

TPN は時間制約を付加したペトリネットの拡張 [24] の 1 つである．システムの信頼性は形式的検証を適用した TPN によって解析することができる．モデル検査法に基づく形式的検証は，システムの大規模な状態を命題変数と実数変数に対する割当によって表現することができる．したがって，この手法に基づく TINA [25] や Romeo [26] 等のツールは複雑で空間を消費する問題に直面する．この問題を解決するため，時間ペトリネットの検証への有界モデル検査 [27] の適用について研究がなされている [28, 29, 30]．有界モデル検査では，状態空間を部分的に記号表現し，論理式の充足可能性判定（SAT）に帰着してその探索を行うことで，状態爆発の影響を軽減することが可能である．

[31] において，著者らは，ペトリネットを対象とした SAT に基づく有界モデル検査法 [32] を拡張した有界モデル検査に基づく TPN に対する検証手法を提案し，既存のモデル検査器に対する有効性が示した．この手法は時間制約を線形制約 (Linear Arithmetic : LA) で表し，検証に対する SMT (Satisfiability Modulo Theories) ソルバの使用を可能にした．この記号表現は，[29] における時間システム (Timed system) の符号化と同様の符号化を採用し，トランジションの発火とプレイス遅延の経過がブール表現として別々に符号化される．著者らは [30] と同様の方法で，差分論理 (Difference Logic：DL) で時間制約を表現するために記号表現を拡張し [33]，DL [34] で記述された式に対する効率的な充足可能性判定アルゴリズムを適用可能にした．

本論文では，DL に基づく符号化の有効性を LA に基づく既存の符号化と比較した比較実験を実施することによって示す．符号化のスケーラビリティを評価するために，異なるサイズの TPN の例題を用いた．また，式サイズの削減 [31] が，提案する符号化に大きな効果をもつことを明らかにした．

以下，本論文の構成を示す．

2 章では，心拍モニタリングに基づく車体制御システムについて述べる．3 章では，非接触機器を用いて心拍間隔を高精度に検出する手法について述べる．4 章では，非接触機器を用いた車載環境での心拍計測に関する実験を行い，その有効性を評価する．5 章では，モデル検査を用いた車体制御システムの検証について述べ，有界および非有界モデル検査ならびに検査対象のモデルである時間ペトリネットについて概説する．6 章では，時間ペトリネットを対象とした有界および非有界モデル検査の適用ならびにその高速化のための技術について述べる．7 章では，提案手法による時間ペトリネットの検証コストについて，適用実験を通して評価する．最後に 8 章で本論文をまとめる．

第 2 章

心拍モニタリングに基づく車体制御システム

2.1　心拍に基づく身体モニタリング尺度

2.1.1　RRI

心臓は，その内部で発生する電気信号によって収縮と膨張を繰り返し，体内の血液を循環させる．この電気信号を記録した心電図は，図 2.1 に示すように，P 波, Q 波, R 波, S 波, T 波, U 波 の 6 つの波から構成される．中でも R 波は心拍を表す指標として用いられ，1 分間に発生する R 波によって心拍数が求められる．R 波の発生間隔を RR 間隔 (RRI : R-R-Interval) と呼び，RRI の変動は自律神経の活動を反映する．自立神経は交感神経と副交感神経に分類される．交感神経が副交感神経より大きく活動すると精神は緊張状態となり，副交感神経が交感神経より大きく活動すると精神は安静状態となる．RRI を周波数解析することで，解析対象者が緊張状態にあるのか安静状態にあるのかを推定することができる，

2.1.2　LF/HF

RRI を周波数解析することで安静状態やストレス状態といった精神状態を推定をすることができる．RRI の周波数解析によって得られたパワースペクトル密度 (Power Spectral Density : PSD) において，0.05 Hz から 0.15 Hz の低周波成分 (Low Frequency : LF) と 0.15 Hz から 0.40 Hz の高周波成分 (High Frequency : HF) は自律神経の状態を表している．HF 成分は安静状態時に活性する副交感神経の活動を表し，LF 成分はストレス

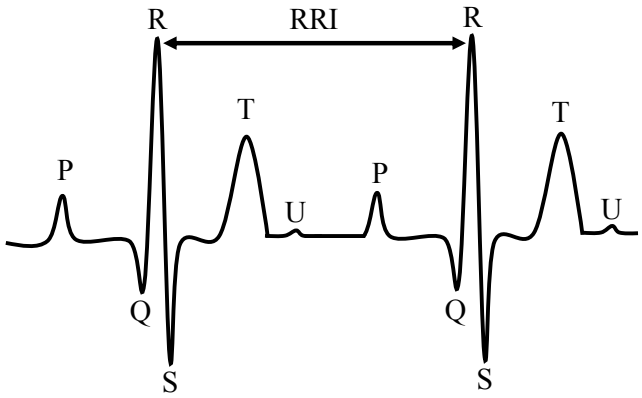


図 2.1　P，Q，R，S，T，U 波および ECG で観測される RRI

状態時に活性する交感神経，および副交感神経の活動を共に表している．LF，HF の大きさは PSD におけるそれぞれの領域の積分値によって得られる．HF は副交感神経の活性度として直接扱え，交感神経の活性度は LF と HF の比 (LF/HF) によって扱うことができる．交感神経の活性度が高まれば LF 成分が増加し，HF 成分は減少するため LF/HF の値は大きくなる．一方，副交感神経の活性度が高まれば LF 成分に対して HF 成分が増加するため LF/HF の値は小さくなる．よって，交感神経の活性度を表す LF/HF は精神状態推定のための指標として用いることができる．

2.2　非接触の身体モニタリング技術

2.2.1　MIMO レーダ

レーダは，対象物へ照射した送信波とその対象物からの反射波の差分を求めることで，対象物までの距離や速度を検知することができる．この特徴を用いることで物体検知にも応用される．しかし，一般にレーダは指向性をもつため検知範囲が制限される．MIMO レーダは送受信を複数のアンテナに分割することによって検知範囲を拡張したレーダである．複数アンテナによって安定した通信を行うことができ，データを分割して送受信することで通信速度の向上にも繋がる．また，複数方向から対象物を捉えることができるため対象の位置特定が可能となる．本研究では 24 GHz ミリ波の MIMO レーダを用いた．ミリ波は波長が mm オーダの電波であり，指向性をもつため互いに干渉することが少ない．環境変化にも強く，天候等の影響を受けずに物体を検知できる特性をもつ．

2.2.2 UWB センサ

UWB は 500 MHz 以上の広帯域の周波数帯を利用する通信を行う無線通信である．UWB ではインパルス (IR : Impulse Radio) 方式に基づく非常に短いパルスを用いて通信を行う．瞬間的にのみパルスが発生するため電波の送受信時刻を高精度に計測でき，さらに単位時間あたりのパルスの密度を高くすることで高速通信を可能とする．これらの特徴を利用することで対象物までの距離を高精度に計測することができる．また，送信する電力密度は低いことが規定されているため低消費電力であり，人体への影響もごく僅かである [35].

以上から UWB センサを心臓に対して用いることで，拍動によるセンサと心臓の距離の変化を高精度に捉えることができ，非接触での心拍検出に利用することができる．

2.3 心拍モニタリングに基づく車体制御

本研究では，心拍モニタリングに基づく車体制御システム（以下，本システム）を提案する．本システムでは，心拍モニタリングの結果を解析して，ドライバへの注意喚起や車体の直接的な制御を行う．心拍のモニタリングには，MIMO レーダや UWB センサなどの非接触型のセンサを用いることで，ドライバへの負担を軽減する．また，運転の安全性を保証する上では車体制御に厳しい時間制約が設けられるため，制御機構をリアルタイムシステムとして設計した上で，モデル検査に基づく形式的検証を行う．このような自動運転を目的としたシステムを対象にモデル検査を用いる場合，その厳しい時間制約の中ではシステムが取り得る状態は膨大となる．したがって，システムが取り得るすべての状態を対象としてモデル検査を適用すると，実用的な時間で検証が終了することは困難となる．そこで本研究では，探索可能な状態を制限することで検証コストを抑えたモデル検査手法の 1 つである有界モデル検査を用いることで，膨大な状態をもつ自動運転システムを扱うことが可能な形式的検証を実現する．

第 3 章

非接触センサを用いた車内における RRI 計測手法の開発

3.1　既存技術における課題

心拍（R 波）を検出する接触型の心拍計測センサは肌に密着し，心臓の拍動に伴う電気信号をセンシングすることで R 波を検出するため，得られる心電図には筋肉からの微弱な電気信号によるノイズ（筋電ノイズ）が加わる程度であり，その後に RRI を計測することも容易である．

一方，非接触型センサによる R 波の検出は離れた位置から行われるため対象の体の揺れ（体動）や外部の環境に由来するノイズが混入する．このようなノイズが大きくなった場合，非接触型センサから得られるデータから直接的に R 波および RRI を計測することは困難である．

したがって，車内での R 波および RRI の計測を考えたとき，接触型のセンサであればその構造上，運転中の車内であっても外部からのノイズを受けず，R 波および RRI を計測できる．しかし，非接触型のセンサを用いた場合，路面状態により車に発生する揺れがノイズとなるため，R 波および RRI の計測が困難となる．

3.2　ノイズフィルタリングによる RRI 計測の高精度化

本研究では，運転中の車内における非接触での RRI 計測を実現するため，前節で述べた問題に対して UWB センサとノイズフィルタリングを組み合わせた RRI の計測を提案する．ノイズフィルタを用いてノイズが含まれるデータから R 波のみを抽出し，その

後 RRI を抽出する．ノイズフィルタにはバンドパスバターワースフィルタ (Bandpass Butterworth Filter) を用いた．バンドパスバターワースフィルタは，指定した周波数の波のみをフィルタリングし，それ以外の周波数の波を減衰させる特性を持った周波数フィルタである．心拍数は通常 1 分間に 60 から 100 回であることに加えて [36] より，1 分間の心拍数の多くが 40 から 100 回の範囲に収まることからバンドパスバターワースフィルタのフィルタリング周波数は 0.67 から 1.67 Hz に設定した．

ここで，心臓は一度電気刺激により拍動すると，以降に最大で 400 msec. 程度は追加の電気信号を受け付けない不応期 [37] と呼ばれる期間をもつ．そのため，不応期中には R 波が発生し得ないという前提のもとに，間隔が 400 msec. より大きい頂点のみを抽出することで，R 波の検出を行う．

以上から，非接触センサによる車内での RRI 計測は以下の手順によって行う．

1. まず，非接触センサを用いて心拍データのセンシングを行う
2. 得られた波形に対してバンドパスバターワースフィルタを用いてノイズの除去を行う
3. さらに，各頂点が 400 msec. 以上の間隔となるように頂点抽出を行う．
4. 得られた頂点から RRI を導出する

上記手順に従って，MIMO レーダまたは UWB センサから得られたデータから RRI を計測する．次章で，接触型の機器に対する MIMO レーダまたは UWB センサの RRI 測定精度を実験を通して評価し，UWB センサが RRI 計測のための非接触センサとしてより有用であることを示す．

第 4 章

非接触センサによる RRI 計測の精度評価

4.1　実験環境

MIMO レーダおよび UWB センサを用いて車内での非接触 RRI 検出が可能かを実験によって確認した．MIMO レーダはサクラテック社製の “miRadar” [38] を用いており，UWB センサはライフセンサー社 [39] による試作機を用いている．車は図 4.1 に示す全長約 300 m の実験コースをおよそ時速 30 km/h で走行した．本実験の目的は，被験者の拍動をセンシングし，RRI 算出に必要なデータを得ることである．よって MIMO レーダは，被験者の胸の高さで，およそ 50 cm 離れた位置に設置し，被験者の拍動が MIMO レーダのセンシング領域に含まれるように設定した．UWB センサは送信出力が低く，電波が微弱であることから，被験者のみぞおちの付近に着衣の上から取り付け，拍動が捉えられるように設定した．また，比較のために既存の接触型心拍検出センサである myBeat [40] を用いた．myBeat は，心臓に流れる電気信号をセンシングすることで直接 RRI を得ることが可能なため，心拍を拍動という物体の動きとしてセンシングする MIMO レーダや UWB センサと比較すると外的要因からの影響を受けにくく，安定した心拍計測が可能である．myBeat は，UWB センサ の取り付け位置との干渉を避けるため，被験者の左胸付近の肌に密着するように取り付けた．以上の実験環境を設定することで MIMO レーダと UWB センサには拍動の信号を含む信号が，送信波と受信波の差分によって得られる．ここで MIMO レーダ，UWB センサ，myBeat のセンシングする際のサンプリング周波数はそれぞれ 25 Hz，1024 Hz，128 Hz である．

車が移動している間のセンサと被験者の位置関係は，車が路面から受ける揺れやカーブ

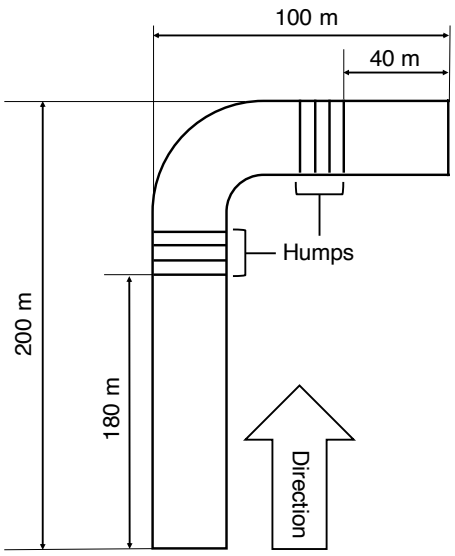


図 4.1　実験コース

での遠心力の影響，また被験者の動きによっても変化する可能性があり，それらはセンシング波形上の変位やノイズとして計測される．MIMO レーダの取り付け位置は被験者の体表面から離れているため，車の揺れが被験者と MIMO レーダに伝搬するまでの時間や強さが異なることから，波形への影響も大きくなる．一方で，UWB センサは被験者の着衣上に直接取り付けられているため，被験者の動きによる衣擦れから生じるセンサとの位置関係の変化は起こり得るものの，車の揺れによる被験者と UWB センサへの影響は，MIMO レーダと比較して小さくなる．

実験は myBeat を比較対象として以下 2 つの実験を実施した．

Exp. 1：　MIMO レーダと myBeat を用いた実験
Exp. 2：　UWB センサと myBeat を用いた実験

4.2　Exp. 1 の結果

図 4.2，図 4.3 は MIMO レーダおよび myBeat から得られた波形である．0 ～ 4 sec. 間は MIMO レーダの動作が安定するために要した時間のため有効なデータとはしていない．図 4.2 では被験者までの距離が大きく，被験者以外の物体からの反射波も受信しているためハンプによる体動ノイズだけでなく，その他の外乱に由来するノイズも重畳している．図 4.3 ではハンプやその他の外乱に関わらず R 波が周期的にスパイク状の波形とし

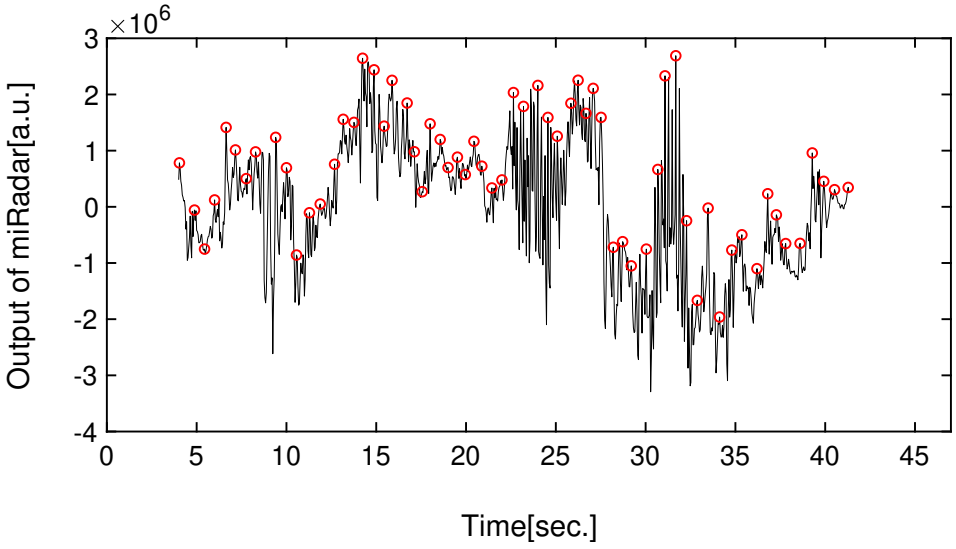


図 4.2　MIMO レーダ によって計測された波形

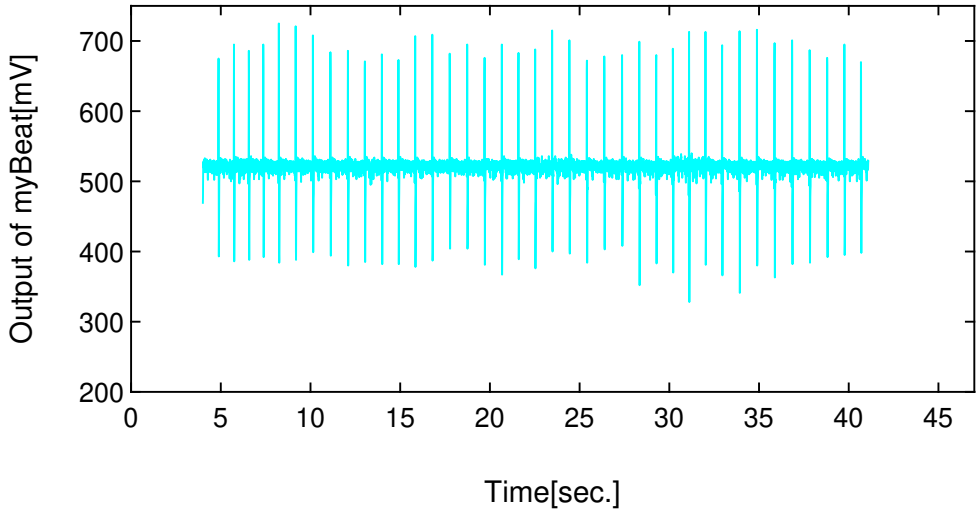


図 4.3　Exp. 1 において myBeat によって計測された波形

て現れている． R 波検出のため 図 4.2 に対してノイズフィルタリングを適用した．ノイズフィルタとしてバンドパスバターワースフィルタを 0.67 ∼ 1.67 Hz の範囲で 図 4.2 の波形に適用し，その後前述の規則を用いて頂点抽出を行なった波形を 図 4.4 に示す．図 4.2 にも同様の頂点抽出を行い，図 4.2 ∼ 4.4 それぞれで検出された R 波を Table 4.1 に示す．Table 4.1 からノイズフィルタリングを施すことにより myBeat の R 波の数に近い値が得られたことが分かる．ここで 図 4.4 と 図 4.3 を重ね合わせ波形を 図 4.5(a) に

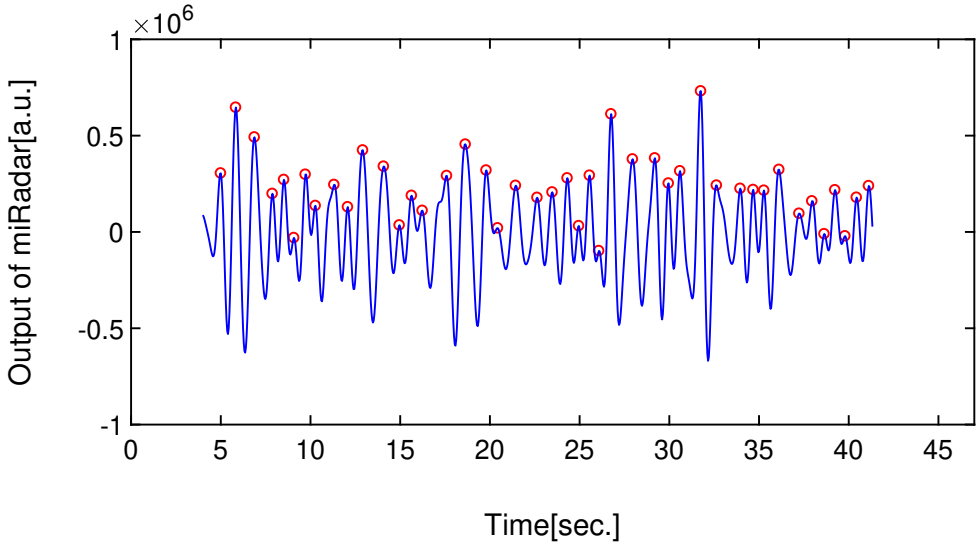
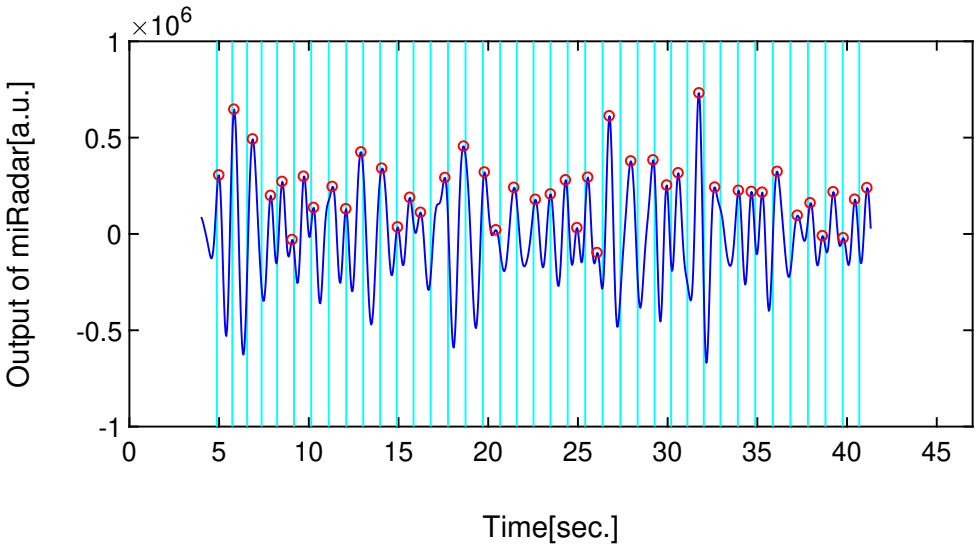
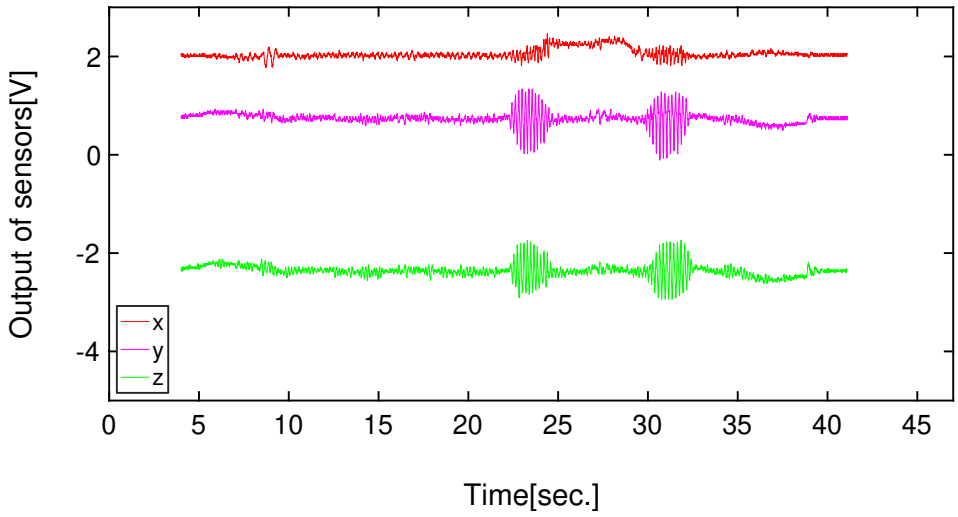


図 4.4　図 4.2 に対してノイズフィルタリングを適用することで得られた波形

示す．図 4.5(a) より myBeat の R 波を検出した付近で MIMO レーダも同様に R 波を検出しているが，myBeat の R 波との隔たりが観られたり，10 sec. 付近および 25 sec. 付近においての R 波の誤検出が観られる．そこで走行中の被験者の動きを myBeat に内蔵された 3 軸の加速度センサを用いてこれらの頂点について考える．加速度センサによって計測された波形を 図 4.5(b) に示す．加速度センサの x，y，z 軸は，車の進行方向に対して左方向が正の変位 (x)，上方向が正の変位 (y)，後方向が正の変位 (z) にそれぞれ対応している．図 4.5(b) より，ハンプに進入したことにより 25 sec. 付近と 30 ∼ 35 sec. 間において各軸の波形が変位している．また，25 sec. ∼ 30 sec. 間で x 軸正方向への変位が見られることから，カーブに進入したことによる遠心力によって，被験者の体が車の進行方向に対して左に傾いていることが分かる．さらに体が傾いたため 10 sec. 付近で x 軸の波形が変化している．したがって，10 sec. 付近と 25 sec. 付近の R 波の誤検出は実験コースや体が傾くことによって発生したノイズによって引き起こされたと考えられる．また，全体としてみられる MIMO レーダと myBeat の R 波のずれは，MIMO レーダと myBeat のセンシング原理および被験者の心臓までの距離とサンプリング周波数が異なるためだと考えられる．MIMO レーダは心臓の動きを検知し，myBeat は心臓を流れる電気信号を検知するため R 波は異なるタイミングで検出される．さらに，MIMO レーダと myBeat のサンプリング周波数は 25 Hz と 128 Hz であるため同じ R 波であっても頂点の位置が異なることや設置位置の距離の違いによって送信波が心臓までに到達する時間が異なることも R 波のずれが生じる要因として挙げられる．



(a) 図 4.4 に 図 4.3 を重ね合わせた波形



(b) Exp. 1 において myBeat の加速度計によって得られた波形

図 4.5　MIMO レーダ と myBeat によって計測された波形の頂点の比較

次に 図 4.4 および 図 4.3 から得られる RRI 波形を 図 4.6 と 図 4.7 にそれぞれ示す．前述したような理由から，図 4.6 は図 4.7 に対して全体として波形が乱れている．

4.3　Exp. 2 の結果

図 4.8，図 4.9 は UWB センサおよび myBeat から得られた波形である． 図 4.8 で

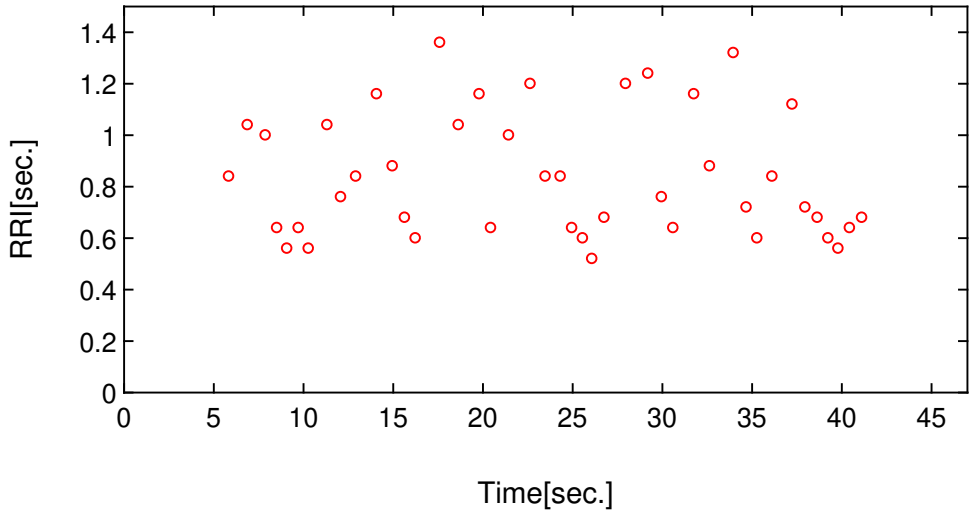


図 4.6　MIMO レーダによって得られた RRI の波形

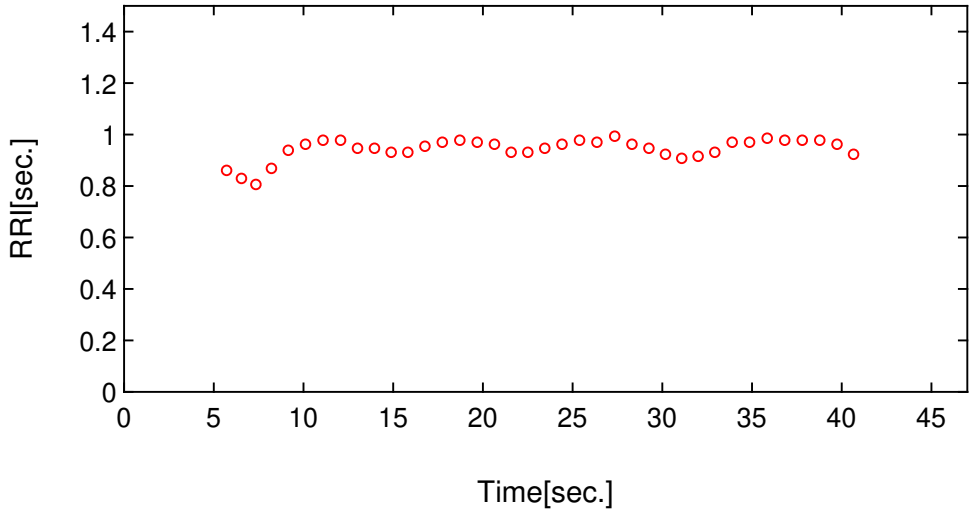


図 4.7　Exp. 1 において myBeat によって得られた RRI の波形

は 25 ～ 30sec. と 35 ～ 40sec. 間にハンプ上を走行しているため体動によるノイズが発生し，波形が乱れていることが分かる．一方， 図 4.9 に示す myBeat から得られた波形は Exp. 1 と同様にハンプを走行中であっても R 波が周期的に現れている． 体動ノイズを取り除くために 図 4.8 の波形に対して Exp. 1 と同様のノイズフィルタリングと頂点抽出を適用した結果を 図 4.10 に示す．図 4.8 にも同様の頂点抽出を行い，図 4.8 ～ 4.10 それぞれで検出された R 波を Table 4.2 に示す．UWB センサのサンプリング周波

表 4.1　Exp. 1 における R 波の数

MIMO レーダ		myBeat
フィルタリング無	フィルタリング有	
64	44	39

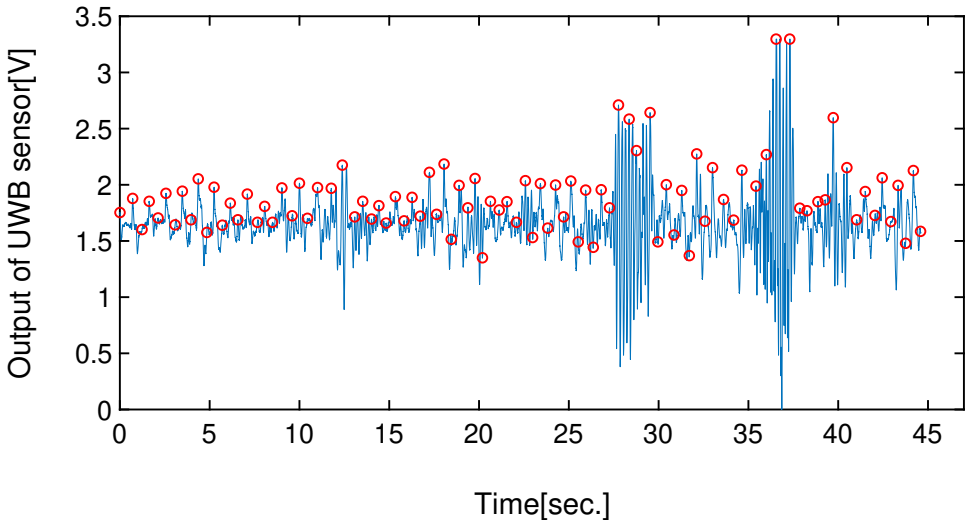


図 4.8　UWB センサによって計測された波形

数は 1024 Hz であり，図 4.8 の頂点を観ると画像上では確認できない微細な頂点も検出している．そのため Table 4.2 から，図 4.2 よりも誤った頂点を検出している．ここで，図 4.9 と 図 4.10 を重ね合わせた図を 図 4.11(a) に示す．図 4.11(a) より，myBeat の R 波との全体的な隔たりがあるものの図 4.5(a) と比較して正確に R 波を検出している．Exp. 1 同様，myBeat の加速度センサの波形を図 4.11(b) に示す．図 4.11(b) より，30 sec. 付近と 35 sec. 付近でハンプによる各軸の変位が観られ，30 sec. ～ 35 sec. 間ではカーブへの進入によって発生した遠心力による x 軸正方向の変位が観られる．さらに 15 sec. 付近でも体が動いたことによって x 軸と y 軸が変位している．結果として，このようなハンプや遠心力による体動ノイズが発生する状況下であっても，図 4.8 ～ 図 4.11 および Table 4.2 から MIMO レーダに比して正確な R 波が検出されている．R 波のずれは MIMO レーダと同様に，UWB センサと myBeat のセンシング原理やサンプリング周波数の違いのよって発生すると考えられる．

次に 図 4.10 および 図 4.9 から得られる RRI 波形を 図 4.12 と 図 4.13 にそれぞれ示す．　myBeat の RRI 波形（図 4.13）に対して UWB の RRI 波形（図 4.12）は バンド

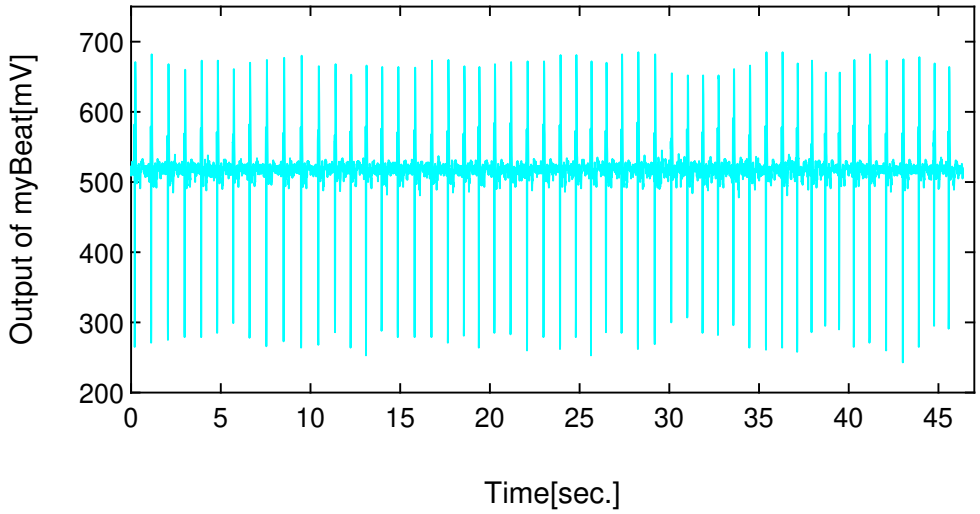


図 4.9　Exp. 2 において myBeat によって計測された波形

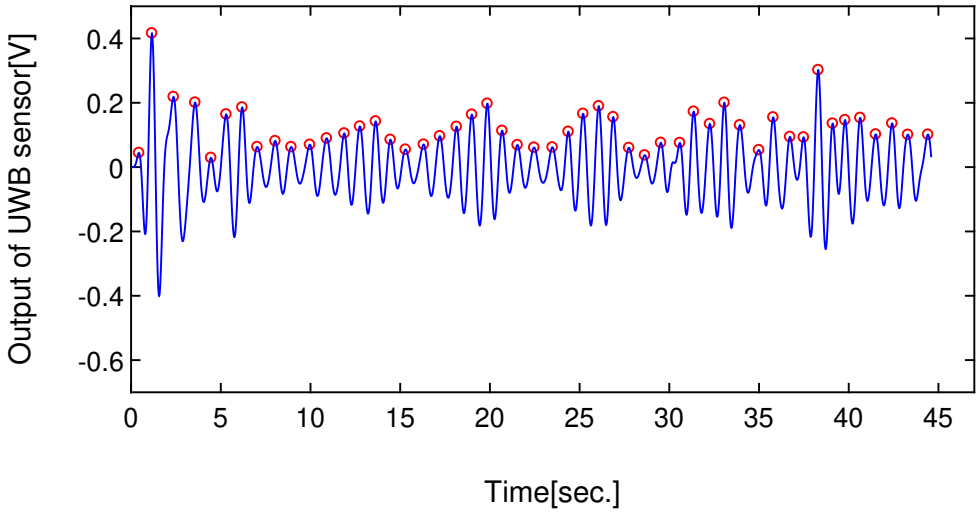
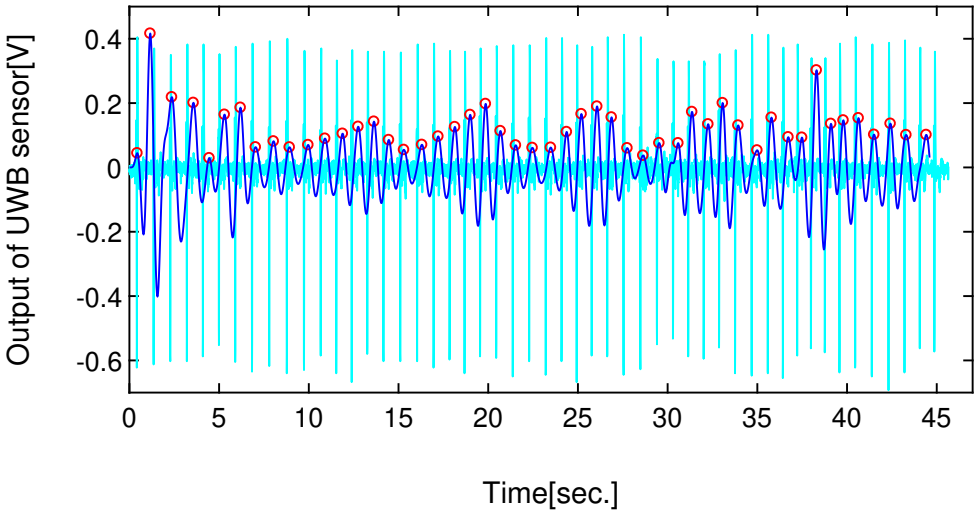
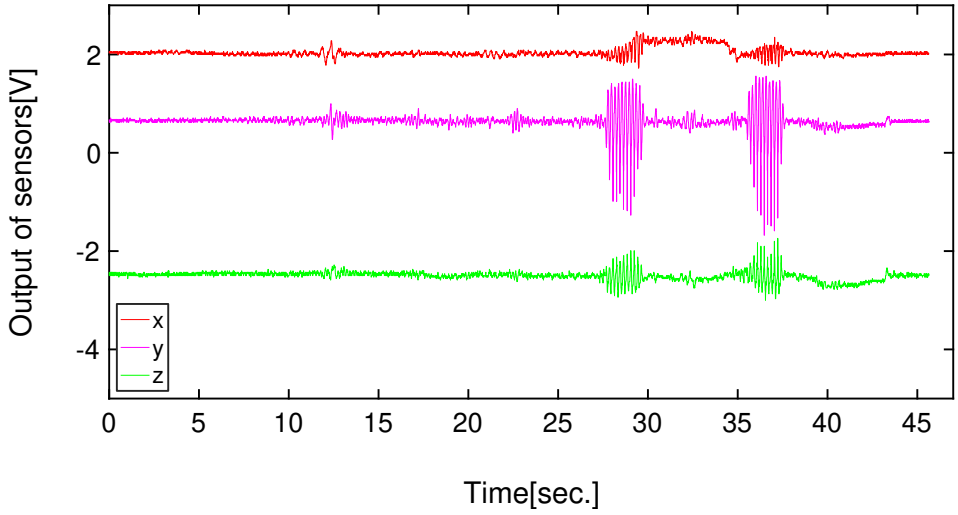


図 4.10　図 4.8 に対してノイズフィルタリングを適用することで得られた波形

パスバターワースフィルタの特性とハンプによる体動により，0 ～ 5 sec. 間と 30 sec. ，35 sec. 付近で波形が乱れている．



(a) 図 4.10 に 図 4.9 を重ね合わせた波形



(b) Exp. 2 において myBeat の加速度計によって得られた波形

図 4.11　UWB センサと myBeat によって計測された波形の頂点の比較

4.4　呼吸による心拍計測の影響

MIMO レーダと UWB センサのセンシングの仕組みから，被験者の呼吸による胸の動きの影響により，得られた波形に呼吸による動きの成分が重畳する可能性が考えられる．特に，MIMO レーダは被験者から離れた位置に設置されているため，呼吸による胸の動

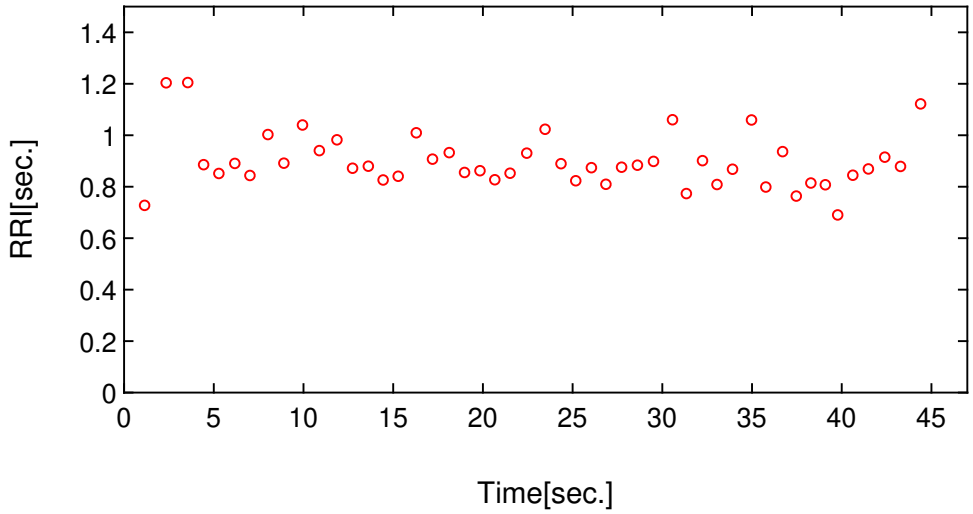


図 4.12　UWB センサから得られた RRI の波形

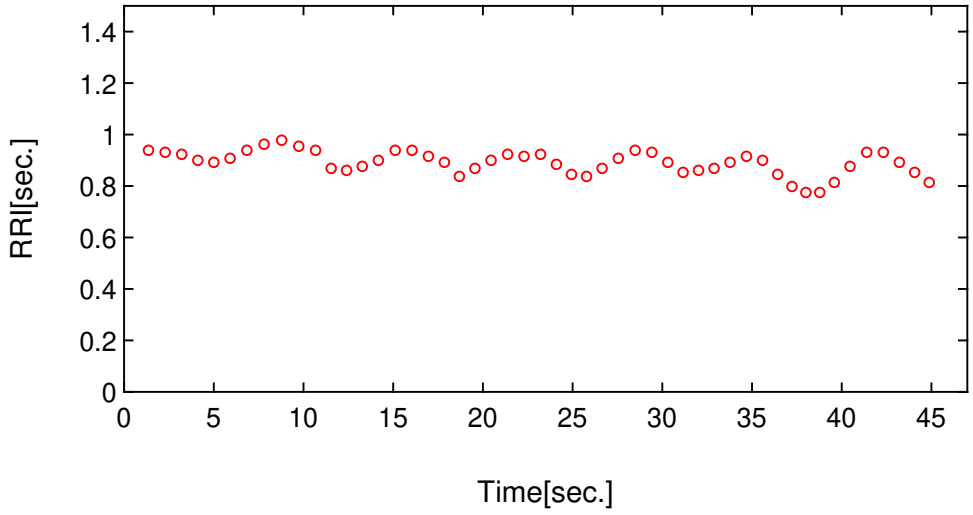


図 4.13　Exp. 2 において myBeat から得られた RRI の波形

きの影響は大きいと予想される．呼気および吸気では胸部がそれぞれ収縮および膨張するため，MIMO レーダとの距離が遠くおよび近くなる．図 4.2 をみると 10 sec. から 15 sec. 間では信号強度が増加傾向にあり，その後 15 sec. から 20 sec. にかけて緩やかに減少傾向に転じている．これは，10 sec. から 15 sec. では吸気が行われ，15 sec. から 20 sec. 間で呼気が行われたためであると推定される．その後の波形ではハンプやカーブによるとみられるノイズの影響が大きく，呼吸による波形への影響を観察することは難し

表 4.2　Exp. 2 における R 波の数

UWB センサ		myBeat
フィルタリング無	フィルタリング有	
93	50	51

い．一方，UWB センサは被験者の服の上に設置しているため，センサが胸と並行して動くことから，胸の動きの信号は抑制されると予想される．図 4.8 をみると，ハンプによるノイズは強く表れているが，MIMO レーダのように呼吸の影響とみられるノイズは観測されなかった．

4.5　Bland-Altman プロットによる計測精度の評価

4.5.1　Bland-Altman プロット

それぞれの機器の RRI 計測の精度を評価するために Bland-Altman プロットを用いた．Bland-Altman プロットは 2 つの測定方法間の一致度を評価するための手法であり，2 つの方法の互換性 (Interchangeability) を検討することができる．

まず，縦軸を 2 つの方法 A，B から得られた測定値 a，b の差 $d = a - b$，横軸に測定値の真値の推測値としてそれらの測定値の平均 $m = (a + b)/2$ をプロットする．2 つの方法から得られた測定値の差の平均 $\bar{d}$ はゼロであることが期待される．また，d が正規分布に従っていると仮定した場合，d の分布の 95 % は d の標準偏差を SD としたときに以下の式によって表される区間に存在する．

$$LOA^u = \bar{d} + 1.96(\simeq 2.00) \times SD \tag{4.1}$$

$$LOA^l = \bar{d} - 1.96(\simeq 2.00) \times SD \tag{4.2}$$

上記の区間は 95 % 一致限界 (Limit Of Agreement : LOA) と呼ばれ，d の誤差区間を表し，方法間の一致の度合いを示す．しかし，上記の LOA は標本集団から得られた区間であるため，母集団に対する LOA ではない．そこで，LOA の標準誤差 SE_{LOA} を用いて 95 % 信頼区間を求めることで，母集団に対する LOA の存在区間を推定する必要がある．信頼区間は標本数を n，t を自由度 $n - 1$ の t 分布における両側 5 % 点の値として以下の式から求められる．

- LOA^l の 95 % 信頼区間

$$LOA^l_{CI^u} = \bar{d} + tSE_{LOA} \tag{4.3}$$
$$LOA^l_{CI^l} = \bar{d} - tSE_{LOA} \tag{4.4}$$
$$※\ SE_{LOA} = \sqrt{3SD^2/n}$$

- LOA^u の 95 % 信頼区間

$$LOA^u_{CI^u} = \bar{d} + tSE_{LOA} \tag{4.5}$$
$$LOA^u_{CI^l} = \bar{d} - tSE_{LOA} \tag{4.6}$$

以上より，式 4.3 ～ 式 4.6 から推定された区間を用いて問題に合わせた誤差区間を設定し，その誤差区間が 2 つの方法が十分に一致していると判断できるほどの許容誤差内に収まっているかどうかで一致度を評価する．本研究では誤差区間として $[LOA^l_{CI^u}, LOA^u_{CI^l}]$ を設定した．

Bland-Altman プロットは比較対象を同一の測定方法の繰り返し測定によって得られた測定値にすることでその測定方法の再現性の評価にも用いることできる．

4.5.2 各機器による RRI 計測精度の評価

myBeat から得られた RRI ($\mathrm{RRI_{myBeat}}$) を比較対象として，MIMO レーダから得られた RRI ($\mathrm{RRI_{MIMO}}$) および UWB センサから得られた RRI ($\mathrm{RRI_{UWB}}$) それぞれの Bland-Altman プロットを 図 4.14，図 4.15 に示す．ここで，Exp. 1 と Exp. 2 の $\mathrm{RRI_{myBeat}}$ を $\mathrm{RRI^1_{myBeat}}$，$\mathrm{RRI^2_{myBeat}}$ とした．$\bar{d}$ を破線で表し，$LOA^l_{CI^u}$ および $LOA^u_{CI^l}$ を一点鎖線で表している．また，各図の $\bar{d}$, $LOA^l_{CI^u}$，$LOA^u_{CI^l}$ の値を Table4.3 に示す．

図 4.15，図 4.14 および Table4.3 より誤差区間 $[LOA^l_{CI^u}, LOA^u_{CI^l}]$ は図 4.14 より 図 4.15 が小さい．したがって，$\mathrm{RRI_{myBeat}}$ に対して $\mathrm{RRI_{UWB}}$ は $\mathrm{RRI_{MIMO}}$ より一致度が高く，$\mathrm{RRI_{myBeat}}$ に近い精度をもつことがわかる．

4.6 RRI から得られる LF/HF の精度

前節で，UWB センサは MIMO レーダより myBeat に近い RRI が得られることを示した．本節では UWB センサの RRI 測定精度が myBeat の RRI 測定精度に対して十分かどうかを LF/HF を用いて評価する．

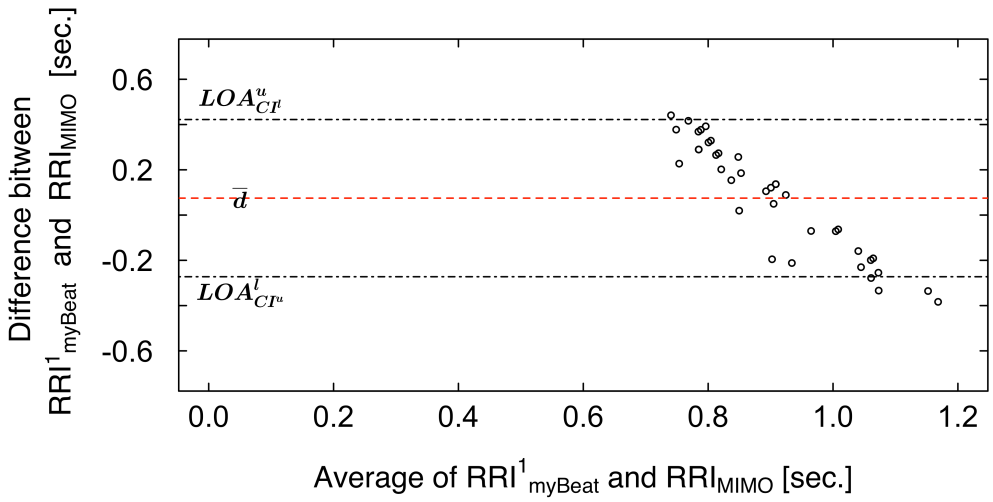


図 4.14　$\mathrm{RRI_{MIMO}}$ と $\mathrm{RRI^1_{myBeat}}$ に対する Bland-Altman プロット

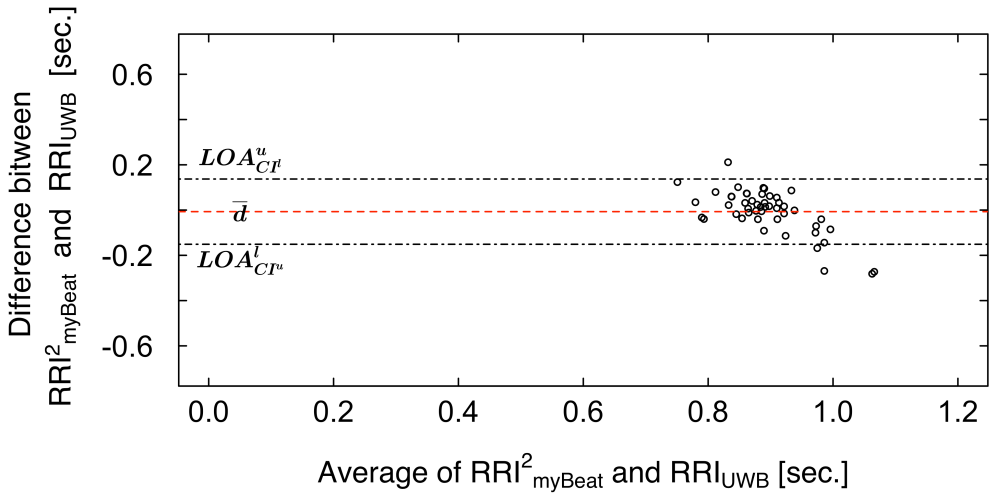


図 4.15　$\mathrm{RRI_{UWB}}$ と $\mathrm{RRI^2_{myBeat}}$ に対する Bland-Altman プロット

図 4.12 と 図 4.13 にプロットされた RRI それぞれに対して周波数解析を実行し，得られた PSD の 0.05 ～ 0.15 Hz と 0.15 ～ 0.40 Hz の領域をそれぞれ積分して LF，HF および LF/HF 求め，求めた LF/HF を表 4.4 に示す．ここで [41] では LF/HF は安静状態時には 2.0 より小さくなり，ストレス状態時には 4.0 以上の値になることが示されている．したがって，表 4.4 に示された LF/HF 間の差は無視できるほど小さい．よって，UWB センサの RRI の測定精度は myBeat の RRI 測定精度に対して十分許容される．

表 4.3　図 4.14 と図 4.15 の Bland-Altman プロットによって得られる $\bar{d}$ と 誤差区間 $[LOA^{l}_{CI^{u}}, LOA^{u}_{CI^{l}}]$ の差異

Bland-Altman プロット	$\bar{d}$	$LOA^{l}_{CI^{u}}$	$LOA^{u}_{CI^{l}}$
図 4.14	0.074	-0.272	0.422
図 4.15	-0.006	-0.151	0.137

表 4.4　図 4.12 と 図 4.13 から得られる LF/HF

図 4.12	図 4.13
0.76656	0.73619

4.7　実験結果

結果として UWB センサを用いることで，既存の接触型機器と同程度な精度で RRI を取得可能であることが示された．よって，運転中の車内において非接触で心拍の変動を観測することが可能となる．心筋梗塞などの心疾患は，その発症に伴って心拍変動がもたらされるため，心拍変動は心疾患の検出に利用することができる．[42] では心筋梗塞について，心拍変動を用いることで 76 % の特異度をもって検出可能であることが述べられている．さらに [43] によると，てんかん (epilepsy) [44] 発作時の約 90 % で心拍変動が観られることが分かっている．したがって，本実験結果から心疾患やてんかん等の心拍変動をもたらす病変の非接触検出が可能であると考えられる．それゆえ運転中の事故防止を目的としたドライバの運転支援の観点においても，本実験結果は有用であると考えられる．

第 5 章

車体制御システムの形式的検証

5.1　モデル検査

モデル検査は，形式的検証の一種で，状態遷移系としてモデル化されたシステムを対象に，その状態空間を網羅的に探索することで，与えられた性質が満たされるか否かを自動的に判定する手法である．特性が満たされない場合，その実行系列が反例として得られる．

モデル検査では，遷移関係を明示的に表現した上で到達可能な全ての状態を探索するため，大規模なシステムに対しては状態数が爆発的に増加し，現実的な時間での検証が困難となる．この問題を状態爆発という．状態爆発問題に有効なモデル検査法の 1 つとして有界モデル検査 [27] が存在する．有界モデル検査は，モデル検査で扱う問題を論理式の充足可能性判定問題に帰着し，SAT ソルバまたは SMT ソルバを用いることで高速な検証を実現する．充足可能性判定問題は，与えれた論理式の各命題変数に対して真偽を割り当て，その論理式全体が真となる割当が存在するかどうかを判定する問題である．論理式の充足可能性は SAT ソルバと呼ばれる充足可能性判定器によって解析される．また，SMT ソルバは SAT ソルバに背景理論を付加した充足可能性判定ツールであり，整数や実数に対する線形制約等を扱うことができる．有界モデル検査では，初期状態から有限長の遷移を表す論理式を構築し，その遷移内で特性を満たすか否かを網羅的に検証する．したがって，明示的な状態空間の探索に基づくモデル検査に比べて状態爆発による検証コストの増大を抑えることができる．

有界モデル検査は探索可能な遷移を制限するため，安全性のような状態空間の全探索が必要な特性を検証することは困難である．そこで，充足不能という結果が得られたときに副次的に生成される補間論理式をもとに，状態空間の上方近似を繰り返し求めることで最

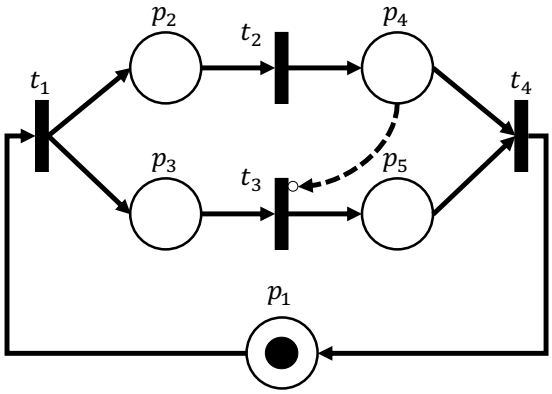


図 5.1　ペトリネットの例

終的に全状態の探索を実現する，非有界モデル検査アルゴリズム [45] が提案されている．非有界モデル検査アルゴリズムを用いることで，SAT および SMT ソルバによる高速な処理と状態空間の網羅的探索を両立したモデル検査が実現できる．

5.2　時間ペトリネット

5.2.1　ペトリネット

ペトリネット $PN = (P, T, F, F_{in}, M_0)$ はプレイスの集合 P，トランジションの集合 T，アークの集合 $F \subseteq (P \times T) \cup (T \times P)$，抑止アークの集合 $F_{in} \subset F$ ，初期マーキング $M_0 \subseteq P$ によって定義される．アークはプレイスとトランジションを接続する有向辺で，あるトランジション $t \in T$ について，t へのアークをもつプレイスを t の入力プレイスという．また，t からのアークをもつプレイスを t の出力プレイスという．プレイスはトークンをもつことができ，トランジションのすべての入力プレイスがトークンをもつときそのトランジションは発火し，出力プレイスへトークンが移動する．抑止アークはプレイスからトランジションへのアークの 1 種であり，抑止アークによって接続されたプレイスがトークンをもつとき，そのトランジションは発火できない．抑止アークからの入力プレイスを抑止プレイスという．初期マーキングは初期状態でトークンをもつプレイスを表す．トランジション $t \in T$ の入力プレイスと出力プレイスはそれぞれ $\bullet t$ と $t\bullet$ と表し，プレイス $p \in P$ の入力トランジションと出力トランジションはそれぞれ $\bullet p$，$p\bullet$ と表す．抑止アークによってトランジションへ接続されたプレイスは $\circ t$ と表す．

図 5.1 にペトリネットの例を示す．トランジション t_1 の入力プレイス $p_1 \in \bullet t_1$ はトークンをもつため，t_1 は発火可能となり即座に発火する．t_1 の発火により t_1 の出力プレイ

ス $p_2, p_3 \in t_1\bullet$ にトークンが移動し，$p_1 \in \bullet t_1$ がもつトークンは失われる．このとき t_2，t_3 はともに発火可能となり，t_2，t_3 のどちらが先に発火するかは非決定的に決まる．t_3 が先に発火した場合，p_5 にトークンが移動する．その後 t_2 が発火することで p_4 にトークンが移動し，t_4 が発火可能となる．そして t_4 の発火によって初期マーキング $M_0 = p_1$ へと戻る．一方 t_2 が先に発火した場合，p_4 にトークンが移動する．p_4 から t_3 へは抑止アークが接続されているため，t_3 が発火するためには p_4 がもつトークンが移動する必要がある．そのためには t_4 が発火する必要があるが，t_4 が発火するためには p_5 がトークンをもたなければならない．したがって，このとき図 5.1 のペトリネットはデッドロックに陥る．

5.2.2 P-TPN

TPN はペトリネットに時間制約を付加したペトリネットの拡張であり，時間制約をペトリネットの要素に特徴付けることで定義される．P-Time Petri Nets (P-TPN) [46] はペトリネットにプレイス遅延を導入した TPN のサブクラスである．P-TPN は 6 組 P-TPN $= (P, T, F, F_{in}, M_0, X)$ により定義され，P はプレイスの集合，T はトランジションの集合，$F \subseteq (P \times T) \cup (T \times P)$ はアークの集合，$F_{in} \subset (P \times T)$ は抑止アークの集合であり，$M_0 \subseteq P$ は初期マーキングを表す．$X : P \to (\mathbb{Z}^+) \times (\mathbb{Z}^+ \cup +\inf)$ はプレイスにプレイス遅延を与える関数であり，$\mathbb{Z}^+$ は 0 以上の整数を表す．ここでは各プレイスが所持できるトークンの数が最大で 1 つの *safe* P-TPN に焦点を当て，アークの重みは考えない．

プレイス遅延はプレイスのトークンが有効になるまでに必要な時間を表し，$p_i \in P$ に対して下界 l_i と上界 u_i $(l_i \leq u_i)$ をもつ．プレイス p_i のトークンは l_i が経過したのちに有効 (*enabled*) となることができ，u_i が経過するまでに有効とならなければならない．トランジションはその入力プレイスすべてが有効なトークンをもつとき，即座に発火しなければならず，発火後はその出力プレイスにトークンが移動する．抑止アークはトランジション発火の抑止を表すために用いられる．抑止アークから入力プレイスによって接続されたトランジションは，その入力プレイスが有効なトークンをもたないときのみ発火できる．

図 5.2 に P-TPN の例を示す．図 5.2 の P-TPN は図 5.1 のペトリネットのプレイスにプレイス遅延を付加した P-TPN である．よって，図 5.2 の P-TPN は図 5.1 のペトリネットの振る舞いにプレイス遅延による時間制約を加えた振る舞いをとる．つまり，各トランジションが発火するためには，その入力プレイスがもつトークンすべてが有効か否

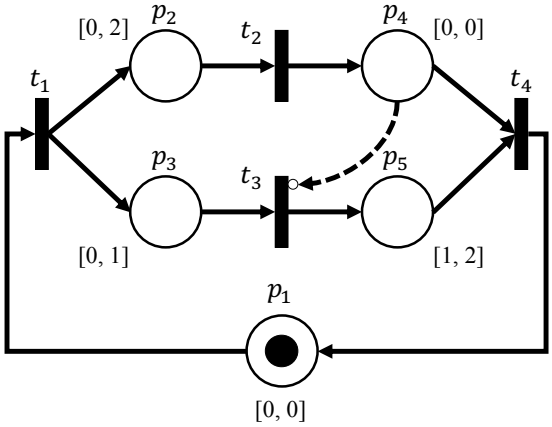


図 5.2　P-TPN の例

かを判定する必要ある．トランジション t_1 の入力プレイス $p_1 \in \bullet t_1$ はトークンをもち，プレイス遅延が $[0,0]$ であるためこのトークンは即座に有効になり，t_1 は発火可能となる．t_1 が発火することで t_1 の出力プレイス $p_2, p_3 \in t_1\bullet$ にトークンが移動し，$p_1 \in \bullet t_1$ がもつトークンは失われる．その後，p_3 がもつトークンが有効になった場合，t_3 が発火し，p_5 にトークンが移動する．続いて p_2 がもつトークンが有効となり，t_2 が発火し，p_4 にトークンが移動する．そして p_3，p_4 がもつトークンが有効となることで t_4 が発火し，初期マーキングへと戻る．一方，p_2 がもつトークンが有効になった場合，t_2 が発火し，p_4 にトークンが移動する．このとき p_4 のプレイス遅延は $[0,0]$ であるため，p_4 がもつトークンは即座に有効となる．したがって，抑止アークにより t_3 は発火不可能となり，デッドロックに陥る．

5.2.3　T-TPN

T-Time Petri Nets (T-TPN) [24] は P-TPN と同様にペトリネット (Petri Nets : PN) にトランジション遅延を導入した TPN のサブクラスである．T-TPN は 6 組 T-TPN $= (P, T, F, M_0, X, w)$ により定義され，P はプレイスの集合，T はトランジションの集合，$F \subseteq (P \times T) \cup (T \times P)$ はアークの集合である．$M_0 : P \to \mathbb{Z}^+$ はプレイスに初期マーキングを与える関数，$X : T \to (\mathbb{Z}^+) \times (\mathbb{Z}^+ \cup +\inf)$ はトランジションにトランジション遅延を与える関数である．ここで $\mathbb{Z}^+$ は 0 以上の整数を表す．$w(p,t)$ および $w(t,p)$ はアーク $(p,t), (t,p) \in F$ に対する重みをそれぞれ表す．

トランジション遅延はトランジションが発火可能になるまでに必要な時間を表し，

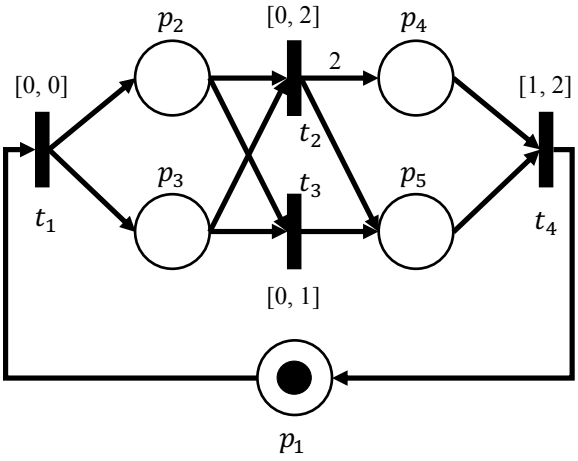


図 5.3　T-TPN の例

$t_j \in T$ に対して下界 l_j と上界 u_j $(l_j \leq u_j)$ をもつ．トランジション t_j について，入力プレイス $\bullet t$ すべてが重み $w(p_i, t_j)$ $(p_i \in \bullet t_j)$ 以上のトークンを得たとき有効となる．有効となってからの経過時間が l_j 以上であれば発火可能であり，u_j が経過するまでに発火しなければならない．発火後は重み $w(t_j, p_h)$ $(p_h \in t_j\bullet)$ に応じた数のトークンが出力プレイス $t_j\bullet$ に移動する．

図 5.3 に T-TPN の例を示す．トランジション t_1 の入力プレイス $p_1 \in \bullet t_1$ はトークンをもち，t_1 のトランジション遅延は $[0, 0]$ であるため t_1 は即座に発火する．その後 p_2，p_3 にトークンが移動し，p_1 のトークンは失われる．このとき t_2 と t_3 はいずれも有効となる．t_2 と t_3 のトランジション遅延はそれぞれ $[0, 2]$，$[0, 1]$ であるため，どちらのトランジションが先に発火するかは非決定的に決まる．t_2 が先に発火した場合，p_4，p_5 にトークンが移動し，p_2，p_3 のトークンは失われる．また，$w(t_2, p_4) = 2$ であるため p_4 は 2 つのトークンを得る．そして t_4 が発火可能となるまでの時間が経過したのちに t_4 が発火することで p_1 にトークンが移動し，p_4，p_5 のトークンは失われる．しかし $w(p_4, t_4) = 1$ であるため，p_4 にはトークンが 1 つ残存する．一方 t_3 が先に発火した場合，p_5 にトークンが移動し，p_2，p_3 のトークンは失われる．このとき 発火可能となるトランジションは存在しないためデッドロックに陥る．

5.3 有界モデル検査

5.3.1 論理式表現

TPN の状態は，プレイスに対するトークンの情報（すなわちマーキング）と経過時間によって表される．l 個のプレイス（すなわち $l = |P|$）をもつ TPN の状態 s は，プレイスのベクトル表現 $\mathbf{p} = (p_1, \cdots, p_l)$（ここで $p_i \in P$）に対する 2 つの l 次ベクトル $\mathbf{m} = (m_1, \cdots, m_l)$ および $\mathbf{x} = (x_1, \cdots, x_l)$ から定義される．m_i は p_i がトークンをもつとき真となる二値変数であり，x_i は p_i が獲得したトークンの経過時間を表す変数である．ここで，状態 s からトランジション t の発火により状態 s' へと遷移することを $s \xrightarrow{t} s'$ と記し，状態 s から時間 x の経過で s' に遷移することを $s \xrightarrow{x} s'$ と記す．状態 s がある集合 S に属しているときかつそのときのみ真となる s の変数上の二値関数 $\mathcal{S}(s)$ を S の特性関数という．同様に，遷移関係の特性関数も，状態 s から s' へ遷移するときかつそのときのみ真となる s および s' の変数上の二値関数 $\mathcal{T}(s, s')$ として定義できる．

SAT に基づく有界モデル検査を実行するためには，2 つの特性関数 $\mathcal{N}_k$ と $\mathcal{R}_k$ への符号化が必要となる [31]．$\mathcal{N}_k(s_0, \cdots, s_k)$ は，初期状態 s_0 が $s_1, s_2, \cdots, s_{k-1}$ を経由して k ステップで s_k に到達可能なことを表す．$\mathcal{R}_k(s_0, \cdots, s_k)$ は，$s_0, \cdots, s_k$ のいずれかの状態で特性が満たされることを表す．初期状態の集合 I の特性関数を $\mathcal{I}(s)$，遷移関係の特性関数を $\mathcal{T}(s, s')$ とすると，$\mathcal{N}_k = \mathcal{I}(s_0) \wedge \mathcal{T}(s_0, s_1) \wedge \cdots \wedge \mathcal{T}(s_{k-1}, s_k)$ と求めることができる．また，$\mathcal{R}_k(s_1, \cdots, s_k)$ は，$s_1, \cdots, s_k$ のいずれかの状態で与えられた特性が満たされることを表す特性関数である．与えられた特性を満たす状態集合 R の特性関数を $\mathcal{R}(s)$ とすると，$\mathcal{R}_k = \mathcal{R}(s_1) \vee \cdots \vee \mathcal{R}(s_k)$ と求めることができる．ここでステップとは，時間経過とトランジション発火によって生じる状態の変化を表す．ステップは，s から状態 s'' を経由して s' へ至る変化として定義される．s は時間経過によって s'' へ変化し，s'' は s' へトランジションの発火によって変化する．有界モデル検査は，システムが初期状態から k ステップ以内に特性を満たすかどうかを，SMT ソルバを用いて $\mathcal{N}_k \wedge \mathcal{R}_k$ の充足可能性を決定することによって検査する．$\mathcal{N}_k \wedge \mathcal{R}_k$ が充足可能なとき，特性は初期状態から k ステップ以内で満たされる．さもなければ，システムは少なくとも k ステップ以内で特性は満たさないことを意味する．

5.3.2 SMT ソルバ

SMT (Satisfiability Modulo Theory) ソルバは充足可能性判定ツールであり，線形制約等の背景理論を扱うことができるため SAT ソルバより高い表現力をもつ．SMT ソルバに入力する命題は SMT-LIB 形式を用いて記述する．SMT ソルバは，論理演算や線形制約などを用いて表現された命題に対して，命題が充足可能であれば **sat** を，充足不能であれば **unsat** を出力する．**sat** の場合は命題を満たす変数への割り当てを出力することができ，また，**unsat** の場合は充足不能となった論理節 (**unsat-core**) を出力することができる．

■基本構文　SMT-LIB 形式ではプログラムの記述に S 式 (S-expression) を採用している．基本的な構文及びコマンドを以下に述べる．

- `(set-option :` *option* `)`：オプション *option* の指定
- `(declare-fun` *name* `()` *type* `)`：変数名 *name*，型 *type* の変数宣言文
- `(assert` *constraint* `)`：命題が満たす制約 *constraint* を記述する誓約文
- `(assert (!` *constraint* `:named` *name* `))`：命題が満たす制約名 *name* の制約 *constraint* を記述する誓約文
- `(check-sat)`：制約 *constraint* を満たす割り当てを求めるコマンド（充足可能性判定の実行）

■例　ブール変数 P，Q 及び整数変数 A からなる論理式 $P \wedge Q \wedge A > 0$ の充足可能性を判定する SMT-LIB プログラムは以下のようになる．

```
> (declare-fun P () Bool)
> (declare-fun Q () Bool)
> (declare-fun A () Int)
> (assert (and P Q (> A 0)))
> (check-sat)
sat
```

`sat` となったときの割り当ては `produce-models` オプションを指定して，`get-value` コマンドを用いると以下のように求められる．

```
> (set-option : produce-mdoels true)
> (declare-fun P () Bool)
> (declare-fun Q () Bool)
> (declare-fun A () Int)
```

```
> (assert (and P Q (> A 0)))
> (check-sat)
sat
> (get-value (P Q A))
  ( (P true)
    (Q true)
    (A 1 ) )
```

一方で，すべての変数がブール変数である論理式 $(P \to Q) \wedge (Q \to R) \wedge (R \to S) \wedge (S \to T) \wedge \neg(Q \to S)$ の充足可能性を判定する SMT-LIB プログラムは以下のようになる．

```
> (declare-fun P () Bool)
> (declare-fun Q () Bool)
> (declare-fun R () Bool)
> (declare-fun S () Bool)
> (declare-fun T () Bool)
> (assert (!  (=> p q) :named PQ))
> (assert (!  (=> q r) :named QR))
> (assert (!  (=> r s) :named RS))
> (assert (!  (=> s t) :named ST))
> (assert (!  (not (=> q s)) :named NQS))
> (check-sat)
> unsat
```

さらに produce-unsat-cores オプションを指定して，get-unsat-core コマンドを用いると充足不能となる論理節を求めることができる．

```
> (set-option :produce-unsat-cores true)
> (declare-fun P () Bool)
> (declare-fun Q () Bool)
> (declare-fun R () Bool)
> (declare-fun S () Bool)
> (declare-fun T () Bool)
> (assert (!  (=> P Q) :named PQ))
> (assert (!  (=> Q R) :named QR))
> (assert (!  (=> R S) :named RS))
> (assert (!  (=> S T) :named ST))
> (assert (!  (not (=> Q S)) :named NQS))
> (check-sat)
> unsat
> (get-unsat-core)
> ( QR
    RS
    NQS )
```

5.4 非有界モデル検査

SAT に基づく有界モデル検査で用いる論理式 $\mathcal{N}_k \wedge \mathcal{R}_k$ は，初期状態から定められた k ステップで与えられた特性を満たす状態へと到達可能であるとき，充足可能となる．前述のように，$\mathcal{N}_k \wedge \mathcal{R}_k$ が充足不能であった場合，少なくとも k ステップ以内で与えられた特性を満たさないことは示されるが，$k+1$ ステップ以上で到達する状態において与えられた特性を満たすか否かについては保証されない．したがって，安全性のように全状態の探索が必要となる特性は，有界モデル検査の枠組みでは検証することができない．

SMT ソルバにより論理式が充足不能と判定されたときに副次的に得られる補間論理式 (interpolation) を用いて状態空間を上方近似することにより，状態空間の全探索を実現する技術が非有界モデル検査である．補間論理式とは，同値でない 2 つの論理式 A，B に対して，$A \wedge B$ が充足不能であるとき得られる，以下の 3 つの条件を満たす論理式 P である．

1. $P \wedge B$ が充足不能である
2. $A \rightarrow P$ が恒真である
3. P は A と B の共通の変数からなる論理式である

ここで，$\mathcal{N}_k \wedge \mathcal{R}_k$ に対して，A および B を以下のようにおくと，$\mathcal{N}_k \wedge \mathcal{R}_k = A \wedge B$ となる．

$$
\begin{aligned}
A =& \mathcal{I}(s_0) \wedge \mathcal{T}(s_0, s_1) \\
B =& \mathcal{T}(s_1, s_2) \wedge \cdots \wedge \mathcal{T}(s_{k-1}, s_k) \wedge (\mathcal{R}(s_1) \vee \cdots \vee \mathcal{R}(s_k))
\end{aligned}
$$

$A \wedge B$ が充足不能であったときに得られる補間論理式 P は条件 3 より状態 s_1 上の論理式となる．また，条件 2 より，P は A を完全に包含する論理式となる．状態 s_0 が初期状態であり，かつ s_0 から s_1 へと 1 ステップで到達するとき，論理式 A は満たされるので，P は初期状態から 1 ステップで到達可能である状態集合の上方近似集合となる．さらに，条件 1 より，P が表す状態からは $k-1$ ステップ以内で求める状態へ到達不可能であることが保証される．

この補間論理式 P を初期状態を表す論理式 $\mathcal{I}$ と置き換えて，再度 SAT ソルバによる充足可能性判定を行う．もし，**unsat** の結果が得られたならば，新たに得られた補間論理式 P' を P と置き換えて充足可能性判定を行う．これを繰り返してゆき，もし $P' = P$ となった場合，P' は P から 1 ステップで到達可能な状態集合の上方近似であるので，

P' は初期状態から到達可能な全ての状態集合の上方近似となるため，条件 1 より求める状態へは到達不可能であることが証明できる．一方，**sat** の結果が得られたのならば，初期状態を近似集合で置き換えていることから，得られた割当ては偽反例の可能性があるため，ステップ数 k を拡大して再度充足可能性判定を行う．以上の手続きを繰り返すことで，求める状態への到達不可能性 (すなわち，安全性) を検証することが可能となる．

第 6 章

時間ペトリネットのモデル検査

6.1 時間ペトリネットの論理式表現

6.1.1 P-TPN の論理式表現

本稿では，TPN における 1 ステップでは，時間経過とトランジション発火が個別に実行されるものと考える．したがって，時間経過による状態変化を表す論理式 $\mathcal{C}(s, d, s')$ とトランジションの発火による状態変化を表す論理式 $\mathcal{F}(s, s')$ により，1 ステップを表す論理関数 $\mathcal{T}(s, d, s')$ は以下のように定義できる．

$$\mathcal{T}(s, d, s') \stackrel{\text{def}}{=} \mathcal{C}(s, d, s'') \wedge \mathcal{F}(s'', s')$$

ここで d は経過した時間を表し，s'' は時間経過とトランジション発火の中間状態を表す．時間経過を表現するため，上述の k ステップを表す特性関数は $\mathcal{N}_k(s_0, \ldots, s_k, d_1, \ldots, d_k)$ へと拡張される．この特性関数は，初期状態から状態 s_k へと k ステップで遷移し，状態 s_{i-1} から状態 s_i への経過時間がそれぞれ d_i となることを表す．また，本稿で示す論理式表現は，relaxed ∃-step semantics [32, 47] に基づいている．すなわち，$\mathcal{T}(s, d, s')$ は，$s = s'$ かつ $d = 0$ であるときも真となるものとする．

トランジション t はすべての入力プレイス $p \in {}^\bullet t$ が有効なトークンをもち，かつすべての抑止プレイス $p \in t^\circ$ が有効なトークンをもたないとき発火可能となる．したがって，t が状態 s で発火可能であることを表す特性関数 $En_t(s)$ は以下のように定義される．

$$En_t(s) \stackrel{\text{def}}{=} \bigwedge_{p_i \in {}^\bullet t} (m_i \wedge u_i \leq x_i) \wedge \bigwedge_{p_i \in t^\circ} \neg(m_i \wedge l_i \leq x_i)$$

一方，t はすべての入力プレイス $p \in {}^\bullet t$ が有効なトークンをもたないか，もしくはある抑止プレイス $p \in t^\circ$ が有効なトークンをもつとき発火不能となる．したがって，t が状態 s

で発火不能であることを表す特性関数 $Ds_t(s)$ は以下のように定義される．

$$Ds_t(s) \stackrel{\text{def}}{=} \bigvee_{p_i \in \bullet t} \neg(m_i \wedge l_i \leq x_i) \vee \bigvee_{p_i \in \circ t} (m_i \wedge u_i \leq x_i)$$

ここで，$En_t(s)$ と $Ds_t(s)$ は互いに排他とはならず，$En_t(s)$ と $Ds_t(s)$ のどちらも満たされない状態 s が存在する．あるトランジション t に対して，$p_i \in \bullet t$ または $p_i \in \circ t$ の経過時間 x_i が $l_i \leq x_i < u_i$ の範囲内にあるとき，p_i のトークンが有効であるか否かは非決定的に決定される．このとき，$En_t(s)$ と $Ds_t(s)$ はどちらも満たされない．

いずれかのトランション t が発火可能なとき，時間経過なくトランジションの発火が実行される．したがって，$\mathcal{C}(s, d, s')$ は以下のように定義される．

$$\begin{aligned}\mathcal{C}(s, d, s') \stackrel{\text{def}}{=} & \bigwedge_{t \in T} \neg En_t(s) \wedge \bigwedge_{p_i \in P} (x'_i = x_i + d \wedge m'_i \leftrightarrow m_i) \wedge d > 0 \\ & \vee \bigwedge_{p_i \in P} (x'_i = x_i \wedge m'_i \leftrightarrow m_i) \wedge d = 0\end{aligned}$$

ここで，m'_i および x'_i は，状態 s' における m_i および x_i の値を表す変数である．

トランジション t に対して，$s \xrightarrow{t} s'$ または $s = s'$ であるときかつそのときのみ真となる特性関数を $F_t(s, s')$ とすると，n 個のトランジション（すなわち $n = |T|$）をもつ TPN のトランジション発火の特性関数 $\mathcal{F}(s, s')$ は以下のように定義される．

$$\mathcal{F}(s, s') \stackrel{\text{def}}{=} F_{t_1}(s, s_1) \wedge F_{t_2}(s_1, s_2) \wedge \cdots \wedge F_{t_n}(s_{n-1}, s')$$

論理式 $F(s, s')$ は，状態 s から $t_1, \ldots, t_n$ という順序でトランジションが発火して状態 s' へと到達するとき，真と評価される．$F_t(s, s')$ は以下のように定義される．

$$\begin{aligned}F_t(s, s') \stackrel{\text{def}}{=} & \neg Ds_t(s) \wedge \bigwedge_{p_i \in t\bullet} (m'_i \wedge x'_i = 0) \\ & \wedge \bigwedge_{p_i \in \bullet t \setminus t\bullet} (\neg m'_i \wedge x'_i = 0) \wedge \bigwedge_{p_i \in P \setminus (\bullet t \cup t\bullet)} (m'_i \leftrightarrow m_i \wedge x'_i = x_i) \\ & \vee \bigwedge_{p_i \in P} (m'_i \leftrightarrow m_i \wedge x'_i = x_i)\end{aligned}$$

以上から，k ステップの遷移を表す論理式 $\mathcal{N}_k$ は以下のように求められる．

$$\begin{aligned}\mathcal{N}_k \stackrel{\text{def}}{=} &\mathcal{I}(s_0) \wedge \mathcal{T}(s_0, d_1, s_{n+1}) \wedge \mathcal{T}(s_{n+1}, d_2, s_{2(n+1)}) \\ &\wedge \cdots \wedge \mathcal{T}(s_{(k-1)(n+1)}, d_k, s_{k(n+1)}) \\ &= \mathcal{I}(s_0) \wedge \mathcal{C}(s_0, d_1, s_1) \wedge F_{t_1}(s_1, s_2) \wedge \cdots \wedge F_{t_n}(s_n, s_{n+1}) \\ &\wedge \cdots \wedge \mathcal{C}(s_{(k-1)(n+1)}, d_k, s_{(k-1)(n+1)+1}) \\ &\wedge F_{t_1}(s_{(k-1)(n+1)+1}, s_{(k-1)(n+1)+2}) \wedge \cdots \wedge F_{t_n}(s_{k(n+1)-1}, s_{k(n+1)})\end{aligned}$$

ここで $\mathcal{I}(s)$ は，初期状態を表す特性関数であり，以下のように定義される．

$$\mathcal{I}(s) = \bigwedge_{p_i \in M_0} m_i \wedge \bigwedge_{p_i \notin M_0} \neg m_i \wedge \bigwedge_{p_i \in P} \wedge x_i = 0$$

求める特性を満たす状態の特性関数があらかじめ $R(s)$ として与えられているものとする．$\mathcal{N}_k$ が満たされ，かつある状態 s_i $(0 \leq i \leq k(n+1))$ において $R(s_i)$ が真となるとき，$\mathcal{C}(s, d, s')$ および $F_t(s, s')$ は $s = s'$ かつ $d = 0$ の場合にも真となるため，$s_{i+1}, \cdots, s_{k(n+1)}$ のすべてに s_i を割り当てたとしても $\mathcal{N}_k$ は真となる．したがって，このとき $\mathcal{N}_k \wedge R(s_{k(n+1)})$ は充足可能となる．一方で，$\mathcal{N}_k \wedge R(s_{k(n+1)})$ が満たされる場合，与えられた特性は k ステップ以内で満たされる．ゆえに，求める特性の特性関数を $\mathcal{R}_k \stackrel{\text{def}}{=} R(s_{k(n+1)})$ として得ることができる．

また，本稿では検証する TPN の特性としてデッドロックを扱う．プレイスのトークンがすべて有効でかつ発火するトランジションが存在しないとき，TPN はデッドロックに陥る．したがって，デッドロックに陥った状態を表す特性関数 $R_d(s)$ は以下のように定義できる．

$$R_d(s) \stackrel{\text{def}}{=} \bigwedge_{t \in T} \neg En_t(s) \wedge \bigwedge_{p_i \in P} (m_i \rightarrow u_i \leq x_i)$$

図 5.2 における 1 ステップ以内にデッドロックが存在するか否かを検証する論理式について考える．検証に用いる論理式は以下のようになる．

$$\begin{aligned}\mathcal{N}_1 \wedge \mathcal{R}_1 = &\mathcal{I}(s_0) \wedge \mathcal{C}(s_0, s_1) \\ &\wedge F_{t_1}(s_1, s_2) \wedge F_{t_2}(s_2, s_3) \wedge F_{t_3}(s_3, s_4) \wedge F_{t_4}(s_4, s_5) \wedge R_d(s_5)\end{aligned}$$

初期マーキングが $M_0 = p_1$ であることから，$\mathcal{I}(s_0)$ は以下のように表される．

$$\begin{aligned}\mathcal{I}(s_0) = &m_1^0 \wedge \neg m_2^0 \wedge \neg m_3^0 \wedge \neg m_4^0 \wedge \neg m_5^0 \\ &\wedge x_1^0 = 0 \wedge x_2^0 = 0 \wedge x_3^0 = 0 \wedge x_4^0 = 0 \wedge x_5^0 = 0\end{aligned}$$

ここで，m_i^j と x_i^j は状態 s_j 上のプレイス p_i に対する変数 m_i，x_i を表す．各トランジション t_i における $En_{t_i}(s_j)$ と $Ds_{t_i}(s_j)$ を以下に示す．

$$
\begin{aligned}
En_{t_1}(s_j) =& (m_1^j \wedge 0 \leq x_1^j) \\
En_{t_2}(s_j) =& (m_2^j \wedge 2 \leq x_2^j) \\
En_{t_3}(s_j) =& (m_3^j \wedge 1 \leq x_3^j) \wedge \neg(m_4^j \wedge 0 \leq x_4^j) \\
En_{t_4}(s_j) =& (m_4^j \wedge 0 \leq x_4^j) \wedge (m_5^j \wedge 2 \leq x_5^j) \\
Ds_{t_1}(s_j) =& \neg(m_1^j \wedge 0 \leq x_1^j) \\
Ds_{t_2}(s_j) =& \neg(m_2^j \wedge 0 \leq x_2^j) \\
Ds_{t_3}(s_j) =& \neg(m_3^j \wedge 0 \leq x_3^j) \vee (m_4^j \wedge 0 \leq x_4^j) \\
Ds_{t_4}(s_j) =& \neg(m_4^j \wedge 0 \leq x_4^j) \vee \neg(m_5^j \wedge 1 \leq x_5^j)
\end{aligned}
$$

よって，$\mathcal{C}$ と F_{t_i} は $En_{t_i}(s_j)$，$Ds_{t_i}(s_j)$ を用いて以下のように構成される．

$$
\begin{aligned}
\mathcal{C}(s_0, s_1) =& \neg En_{t_1}(s_0) \wedge \neg En_{t_2}(s_0) \wedge \neg En_{t_3}(s_0) \wedge \neg En_{t_4}(s_0) \\
& \wedge (x_1^1 = x_1^0 + d \wedge m_1^1 \leftrightarrow m_1^0) \\
& \wedge (x_2^1 = x_2^0 + d \wedge m_2^1 \leftrightarrow m_2^0) \\
& \wedge (x_3^1 = x_3^0 + d \wedge m_3^1 \leftrightarrow m_3^0) \\
& \wedge (x_4^1 = x_4^0 + d \wedge m_4^1 \leftrightarrow m_4^0) \\
& \wedge (x_5^1 = x_5^0 + d \wedge m_5^1 \leftrightarrow m_5^0) \\
& \vee ((m_1^1 \leftrightarrow m_1^0 \wedge x_1^1 = x_1^0) \wedge (m_2^1 \leftrightarrow m_2^0 \wedge x_2^1 = x_2^0) \\
& \wedge (m_3^1 \leftrightarrow m_3^0 \wedge x_3^1 = x_3^0) \wedge (m_4^1 \leftrightarrow m_4^0 \wedge x_4^1 = x_4^0) \\
& \wedge (m_5^1 \leftrightarrow m_5^0 \wedge x_5^1 = x_5^0))
\end{aligned}
$$

$$
\begin{aligned}
F_{t_1}(s_1,s_2) =& \neg Ds_{t_1}(s_1) \wedge (m_2^2 \wedge x_2^2 = 0) \\
& \wedge (m_3^2 \wedge x_3^2 = 0) \wedge (\neg m_1^2 \wedge x_1^2 = 0) \\
& \wedge (m_4^2 \leftrightarrow m_4^1 \wedge x_4^2 = x_4^1) \wedge (m_5^2 \leftrightarrow m_5^1 \wedge x_5^2 = x_5^1) \\
& \vee ((m_1^2 \leftrightarrow m_1^1 \wedge x_1^2 = x_1^1) \wedge (m_2^2 \leftrightarrow m_2^1 \wedge x_2^2 = x_2^1) \\
& \wedge (m_3^2 \leftrightarrow m_3^1 \wedge x_3^2 = x_3^1) \wedge (m_4^2 \leftrightarrow m_4^1 \wedge x_4^2 = x_4^1) \\
& \wedge (m_5^2 \leftrightarrow m_5^1 \wedge x_5^2 = x_5^1)) \\
F_{t_2}(s_2,s_3) =& \neg Ds_{t_2}(s_2) \wedge (m_4^3 \wedge x_4^3 = 0) \wedge (\neg m_2^3 \wedge x_2^3 = 0) \\
& \wedge (m_1^3 \leftrightarrow m_1^2 \wedge x_1^3 = x_1^2) \wedge (m_3^3 \leftrightarrow m_3^2 \wedge x_3^3 = x_3^2) \\
& \wedge (m_5^3 \leftrightarrow m_5^2 \wedge x_5^3 = x_5^2) \\
& \vee ((m_1^3 \leftrightarrow m_1^2 \wedge x_1^3 = x_1^2) \wedge (m_2^3 \leftrightarrow m_2^2 \wedge x_2^3 = x_2^2) \\
& \wedge (m_3^3 \leftrightarrow m_3^2 \wedge x_3^3 = x_3^2) \wedge (m_4^3 \leftrightarrow m_4^2 \wedge x_4^3 = x_4^2) \\
& \wedge (m_5^3 \leftrightarrow m_5^2 \wedge x_5^3 = x_5^2)) \\
F_{t_3}(s_3,s_4) =& \neg Ds_{t_3}(s_3) \wedge (m_5^4 \wedge x_5^4 = 0) \wedge (\neg m_3^4 \wedge x_3^4 = 0) \\
& \wedge (m_1^4 \leftrightarrow m_1^3 \wedge x_1^4 = x_1^3) \wedge (m_2^4 \leftrightarrow m_2^3 \wedge x_2^4 = x_2^3) \\
& \wedge (m_4^4 \leftrightarrow m_4^3 \wedge x_4^4 = x_4^3) \\
& \vee ((m_1^4 \leftrightarrow m_1^3 \wedge x_1^4 = x_1^3) \wedge (m_2^4 \leftrightarrow m_2^3 \wedge x_2^4 = x_2^3) \\
& \wedge (m_3^4 \leftrightarrow m_3^3 \wedge x_3^4 = x_3^3) \wedge (m_4^4 \leftrightarrow m_4^3 \wedge x_4^4 = x_4^3) \\
& \wedge (m_5^4 \leftrightarrow m_5^3 \wedge x_5^4 = x_5^3)) \\
F_{t_4}(s_4,s_5) =& \neg Ds_{t_4}(s_4) \wedge (m_1^5 \wedge x_1^5 = 0) \\
& \wedge (\neg m_4^5 \wedge x_4^5 = 0) \wedge (\neg m_5^5 \wedge x_5^5 = 0) \\
& \wedge (m_1^5 \leftrightarrow m_1^4 \wedge x_1^5 = x_1^4) \wedge (m_2^5 \leftrightarrow m_2^4 \wedge x_2^5 = x_2^4) \\
& \wedge (m_3^5 \leftrightarrow m_3^4 \wedge x_3^5 = x_3^4) \\
& \vee ((m_1^5 \leftrightarrow m_1^4 \wedge x_1^5 = x_1^4) \wedge (m_2^5 \leftrightarrow m_2^4 \wedge x_2^5 = x_2^4) \\
& \wedge (m_3^5 \leftrightarrow m_3^4 \wedge x_3^5 = x_3^4) \wedge (m_4^5 \leftrightarrow m_4^4 \wedge x_4^5 = x_4^4) \\
& \wedge (m_5^5 \leftrightarrow m_5^4 \wedge x_5^5 = x_5^4))
\end{aligned}
$$

最後に R_d を以下のように得る．

$$
\begin{aligned}
R_d(s_5) =& \neg En_{t_1}(s_5) \wedge \neg En_{t_2}(s_5) \wedge \neg En_{t_3}(s_5) \wedge \neg En_{t_4}(s_5) \\
& \wedge (m_1^5 \rightarrow 0 \leq x_1^5) \wedge (m_2^5 \rightarrow 2 \leq x_2^5) \wedge (m_3^5 \rightarrow 1 \leq x_3^5) \\
& \wedge (m_4^5 \rightarrow 0 \leq x_4^5) \wedge (m_5^5 \rightarrow 2 \leq x_5^5)
\end{aligned}
$$

したがって，$\mathcal{N}_k \wedge \mathcal{R}_k$ の充足可能性を判定することで，図 5.2 の P-TPN が 1 ステップ

でデッドロックに到達可能か否かを検証することができる．

6.1.2 T-TPN の論理式表現

P-TPN では，トークンが有効であるか否かが都度評価される．そのため各プレイスが獲得可能なトークンの上限が明らかではない P-TPN では，プレイスが複数のトークンをもつとき，その各トークンごとの経過時間を個別に管理する必要がある．したがって，このような P-TPN を有界モデル検査で扱う場合，プレイスが獲得しているトークンの数に応じてそのトークンの経過時間を表すための変数を動的に確保する必要がある．しかし前述した P-TPN の論理式表現のための枠組みでは，変数は静的に決定しなければならない．ゆえに，このような P-TPN に対して有界モデル検査を適用することは困難である．一方，T-TPN はトランジションに対して時間遅延が特徴付けられているため，各トランジションにおいて経過した時間を表すために必要な変数は静的に決定する．ここでは，
各プレイスが獲得可能なトークンの上限が明らかではない TPN を有界モデル検査で扱うために T-TPN の論理式表現を考える．

P-TPN の論理式表現と同様の考えを用いて，時間経過による状態変化を表す論理式 $\mathcal{C}(s, s')$ とトランジションの発火による状態変化を表す論理式 $\mathcal{F}(s, s')$ により，1 ステップを表す論理関数 $\mathcal{T}(s, s')$ は以下のように定義する．

$$\mathcal{T}(s, s') \stackrel{\text{def}}{=} \mathcal{C}(s, s'') \wedge \mathcal{F}(s'', s')$$

s'' は時間経過とトランジション発火の中間状態を表し，また $\mathcal{T}(s, s')$ は，$s = s'$ であるときも真となるものとする．

T-TPN の状態 s は，$\mathbf{p} = (p_1, \cdots, p_l)$ とトランジション $\mathbf{t} = (t_1, \cdots, t_n)$ に対する 2 つの l 次ベクトル $\mathbf{m} = (m_1, \cdots, m_l)$ および $\mathbf{z} = (z_1, \cdots, z_n)$ と，大域的な時刻を表す変数 c によって定義される．m_i は p_i がもつトークンの数を表す整数変数である．z_j は t_j が有効となってからの経過時間を表す変数であり，その時点での c の値が格納される．

これらの変数を用いて，マーキング M に対してトランジション t が有効であるときかつそのときのみ真となる論理式を以下のように定義できる．

$$En(M, t) \stackrel{def}{=} \bigwedge_{p_i \in {}^\bullet t} m_i \geq w(p_i, t)$$

時間経過は，すべての有効なトランジションの経過時間が上界以下であれば実行可能で

ある．したがって，時間経過を表す特性関数は以下のように定義される．

$$\begin{aligned}\mathcal{C}(s,s') \stackrel{def}{=} & (c'-c>0)\\ & \wedge \bigwedge_{t_j\in T}\Big(En(M,t_j)\rightarrow (c'-z_j)\leq u_j\Big)\wedge (z'_j-z_j=0)\\ & \wedge \bigwedge_{p_i\in P}(m'_i-m_i=0)\\ & \vee (c'-c=0)\wedge \bigwedge_{t_j\in T}(z'_j-z_j=0)\wedge \bigwedge_{p_i\in P}(m'_i-m_i=0)\end{aligned}$$

ここで，m'_i，z'_i および c' は，状態 s' における m_i，z_i および c の値を表す変数である．

状態 s でトランジション t_k が発火するためには，s で発火可能である必要がある．また，t_k の発火によって t_k の出力プレイスの出力トランジション $(t_k\bullet)\bullet$ が有効となる場合がある．したがって，トランジション発火を表す特性関数は以下のように定義される．

$$\begin{aligned}F_{t_k}(s,s') \stackrel{def}{=} & (c'-c=0)\\ & \wedge (c-z_k\geq l_k)\wedge En(M,t_k)\wedge (En(M',t_k)\rightarrow (z'_k-c'=0))\\ & \wedge \bigwedge_{p_i\in(\bullet t_k\cup t_k\bullet)}\Big(m'-m_i=w(t_k,p_i)-w(p_i,t_k)\Big)\\ & \wedge \bigwedge_{p_i\in P\setminus(\bullet t_k\cup t_k\bullet)}(m'_i-m_i=0)\\ & \wedge \bigwedge_{t_j\in(t_k\bullet)\bullet}\Big((En(M',t_j)\wedge\neg En(M,t_j))\rightarrow (z'_j-c=0)\Big)\\ & \qquad\wedge\Big(\neg(En(M',t_j)\wedge\neg En(M,t_j))\rightarrow (z'_j-z_j=0)\Big)\\ & \wedge \bigwedge_{t_j\in T\setminus((t_k\bullet)\bullet\cup t_k)}(z'_j-z_j=0)\\ & \vee (c'-c=0)\wedge \bigwedge_{p_i\in P}(m'_i-m_i=0)\wedge \bigwedge_{t_j\in T}(z'_j-z_j=0)\end{aligned}$$

ここで，M' は s' における M を表す．

T-TPN において，すべてのトランジションが有効でなければデッドロックとなる．よって，デッドロックを表す特性関数は以下のように定義される．

$$R_d(s)\stackrel{def}{=}\bigwedge_{t_j\in T}\neg En(M,t_j)$$

また，初期状態を表特性関数は以下のように定義される．

$$\mathcal{I}(s) \stackrel{def}{=} (c=0) \wedge \bigwedge_{p_i \in P} M_0(p_i) \wedge \bigwedge_{t_j \in T} \Big(En(M, t_j) \rightarrow (z_j - c = 0) \Big)$$

6.2 検証コストの削減

6.2.1 差分論理を用いた高速化

SMT ソルバは，線形制約に基づく論理式の充足可能性を判定することができる．線形制約は，変数 $v_1, v_2, \cdots, v_n$ と係数 $a_1, a_2, \cdots, a_n$ および定数 c に対して，

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \bowtie c \quad (\text{ここで，} \bowtie \in \{=, \neq, \leq, <, \geq, >\})$$

という形の不等式として与えられる．一方で差分論理は線形制約の部分論理であり，その不等式は変数 x および y と定数 c に対して，

$$x - y \bowtie c \quad (\text{ここで，} \bowtie \in \{=, \neq, \leq, <, \geq, >\})$$

という形に限定される．

差分論理として与えられた問題に対しては，それを重み付きの有向グラフに変換し，重みの総和が負となる閉路（negative loop）を探索することで解の有無が判定できる [34]. このグラフでは，変数が頂点となり，それぞれの制約 $x - y > c$ に対して，頂点 x から頂点 y へ重み c をもつ有向辺が接続される．これにより，線形制約の解の探索をグラフの閉路探索に帰着して解くことができ，高速な処理が可能となる．

例として，以下の 4 つの制約が与えられた場合を考える．

$$\begin{aligned} x - y &\leq 1 \\ z - x &\leq -1 \\ y - z &\leq 2 \\ x - z &\leq -2 \end{aligned}$$

このとき，この 4 つの制約からは図 6.1 のように 3 つの頂点と 4 の辺をもつグラフが構成される．グラフから，頂点 x から頂点 z の間に重みの総和が負となる閉路が存在することがわかる．したがって，この 4 つの制約を満たす解は存在しないことがわかる．

前節で示した P-TPN の論理式表現（以降，従来表現という）では，プレイス遅延による時間の経過は $x' = x + d \wedge d > 0$ という不等式として表現される．この不等式は，トークンを獲得してからの経過時間を表す変数 x および x' と，経過時間を表す変数 d の 3

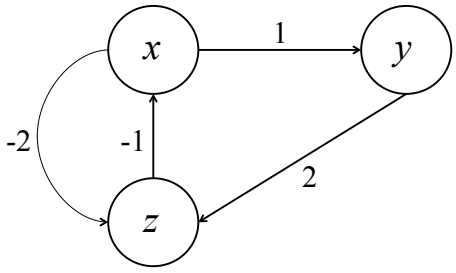


図 6.1　線形制約から得られるグラフ

つの変数をもつため，線形制約上の不等式となる．差分論理上の不等式としてこの制約を表現するため，提案する論理式表現（以降，提案表現という）では，各プレイスにおける遅延をトークンを獲得してからの経過時間ではなく，トークンを獲得した時刻によって表現する．

提案表現では，TPN の状態 s は，$\mathbf{p} = (p_1, \cdots, p_l)$ に対する 2 つの l 次ベクトル $\mathbf{m} = (m_1, \cdots, m_l)$ および $\mathbf{z} = (z_1, \cdots, z_l)$ と，大域的な時刻を表す変数 c によって定義される．m_i は従来表現と同じく p_i がトークンをもつとき真となる二値変数である．z_i は p_i がトークンを獲得した時刻を表す変数であり，トークンを獲得した時点での c の値が格納される．これにより，プレイス遅延による時間の経過は $z' = z \wedge c' - c > 0$ という不等式として表現できる．この不等式はいずれの項も 2 つの変数しかもたないため，差分論理上の不等式となる．

上述の変数を用いて，トランジション t が状態 s で発火可能および発火不能であることを表す差分論理上の特性関数 $En_t^{DL}(s)$ および $Ds_t^{DL}(s)$ はそれぞれ以下のように定義できる．

$$En_t^{DL}(s) \stackrel{\text{def}}{=} \bigwedge_{p_i \in \bullet t} (m_i \wedge u_i \leq c - z_i) \wedge \bigwedge_{p_i \in \circ t} \neg(m_i \wedge l_i \leq c - z_i)$$

$$Ds_t^{DL}(s) \stackrel{\text{def}}{=} \bigvee_{p_i \in \bullet t} \neg(m_i \wedge l_i \leq c - z_i) \vee \bigvee_{p_i \in \circ t} (m_i \wedge u_i \leq c - z_i)$$

各プレイス p_i におけるトークン経過時間とプレイス遅延の上限および下限に関する不等式（$u_i \leq c - z_i$ および $l_i \leq c - z_i$）も，差分論理上の不等式として同様に表現できる．

次に，時間経過による状態 s から状態 s' への変化を表す差分論理上の特性関数

$C^{DL}(s,s')$ は以下のように定義できる．

$$\mathcal{C}^{DL}(s,s') \stackrel{\text{def}}{=} \bigwedge_{t\in T} \neg En_t^{DL}(s) \wedge \bigwedge_{p_i\in P} (z_i' = z_i \wedge m_i' \leftrightarrow m_i) \wedge (c' - c > 0)$$
$$\vee \bigwedge_{p_i\in P} (z_i' = z_i \wedge m_i' \leftrightarrow m_i) \wedge (c' - c = 0)$$

ここで，従来表現と同様に m_i'，z_i'，c' は 状態 s' における m_i，z_i，c をそれぞれ表す．上述のとおり，プレイス遅延による時間の経過を表す論理式を差分論理上の不等式として表現できる．

最後に，TPN のトランジション発火を表す差分論理上の特性関数 $F^{DL}(s,s')$ は以下のように定義できる．

$$\mathcal{F}^{DL}(s,s') \stackrel{\text{def}}{=} F_{t_1}^{DL}(s,s_1) \wedge F_{t_2}^{DL}(s_1,s_2) \wedge \cdots \wedge F_{t_n}^{DL}(s_{n-1},s')$$

ここで，トランジション t の発火を表す差分論理上の特性関数 $F_t^{DL}(s,s')$ は以下のように定義される．

$$F_t^{DL}(s,s') \stackrel{\text{def}}{=} \neg Ds_t^{DL}(s) \wedge \bigwedge_{p_i\in t\bullet} (m_i' \wedge z_i' = c) \wedge (c' - c = 0)$$
$$\wedge \bigwedge_{p_i\in \bullet t\setminus t\bullet} (\neg m_i' \wedge z_i' = z_i) \wedge \bigwedge_{p_i\in P\setminus(\bullet t\cup t\bullet)} (m' \leftrightarrow m_i \wedge z_i' = z_i)$$
$$\vee \bigwedge_{p\in P} (m_i' \leftrightarrow m_i \wedge z_i' = z_i) \wedge (c' - c = 0)$$

得られた $\mathcal{C}^{DL}(s,s')$ および $\mathcal{F}^{DL}(s,s')$ を用いて，1 ステップを表す特性関数 $\mathcal{T}^{DL}(s,s')$ は以下のように定義できる．

$$\mathcal{T}^{DL}(s,s') \stackrel{\text{def}}{=} \mathcal{C}^{DL}(s,s'') \wedge \mathcal{F}^{DL}(s'',s')$$

さらに，デッドロックに陥った状態を表す特性関数 $R_d^{DL}(s)$ は以下のように定義できる．

$$R_d^{DL}(s) \stackrel{\text{def}}{=} \bigwedge_{t\in T} \neg En_t^{DL}(s) \wedge \bigwedge_{p_i\in P} (m_i \rightarrow u_i \leq c - x_i)$$

また，$\mathcal{I}^{DL}(s)$ は初期状態の特性関数を表し，以下のように定義される．

$$\mathcal{I}^{DL}(s) \stackrel{def}{=} c = 0 \wedge \bigwedge_{p_i\in M_0} m_i \wedge \bigwedge_{p_i\notin M_0} \neg m_i \wedge \bigwedge_{p_i\in P} z_i = 0$$

以上のように，差分論理に基づく TPN の論理式表現が可能となる．

6.2.2　変数削減による高速化

従来表現と提案表現のいずれもステップ数が増加すると論理式の規模が大きくなるため，充足可能性判定にかかるコストも増加する．[31] では，変化しない変数を置換することによって論理式のサイズを削減するための手法が述べられている．$\mathcal{N}_k \wedge \mathcal{R}_k$ は充足可能性を保持したまま簡略化することができ，判定にかかるコストを削減することができる．この簡略化は $f(x,y,z) = g(x,y,z) \wedge (y = z)$ の形をした論理式に対して行うことができる．f, g は論理関数である．z を y に置き換えると $f(x,y,z)$ の充足可能性を保持しつつ以下のように変換できる．

$$f(x,y,y) = g(x,y,y)$$

よって，$(y = z)$ が削除され，変数も (x,y,z) から (x,y) に削減される．

従来表現と提案表現での論理式表現に対する変数削減の適用について述べる．変数削減の適用対象となるのは従来表現，提案表現ともに時間経過を表す論理式 $\mathcal{C}(s,d,s')$，$\mathcal{C}^{DL}(s,s')$ 及びトランジション t による発火を表す論理式 $\mathcal{F}_t(s,s')$，$F_t^{DL}(s,s')$ である．

■従来表現の変数削減　$\mathcal{C}$，F_t からそれぞれ共通する部分論理式を括り出す．

$$\begin{aligned}
\mathcal{C}(s,d,s') \stackrel{\text{def}}{=} & \left(\bigwedge_{t \in T} \neg En_t(s) \wedge \bigwedge_{p_i \in P} (x_i' = x_i + d) \wedge d > 0 \vee \bigwedge_{p_i \in P} (x_i' = x_i) \wedge d = 0 \right) \\
& \wedge \bigwedge_{p_i \in P} (m_i' \leftrightarrow m_i) \\
F_t(s,s') \stackrel{\text{def}}{=} & \left(\neg Ds_t(s) \wedge \bigwedge_{p_i \in t\bullet} (m_i' \wedge x_i' = 0) \wedge \bigwedge_{p_i \in \bullet t \setminus t\bullet} (\neg m_i' \wedge x_i' = 0) \right. \\
& \left. \vee \bigwedge_{p_i \in (\bullet t \cup t\bullet)} (m_i' \leftrightarrow m_i \wedge x_i' = x_i) \right) \\
& \wedge \bigwedge_{p_i \in P \setminus (\bullet t \cup t\bullet)} (m_i' \leftrightarrow m_i \wedge x_i' = x_i)
\end{aligned}$$

よって，Algorithm1 に示すアルゴリズムに従って共通部分を削除して変数の置き換え

を行うことで以下の論理式に削減される．

$$\tilde{\mathcal{C}}(s,d,s') \stackrel{\text{def}}{=} \bigwedge_{t\in T} \neg En_t(s) \wedge \bigwedge_{p_i\in P} (x'_i = x_i + d) \wedge d > 0 \vee \bigwedge_{p_i\in P} (x'_i = x_i) \wedge d = 0$$

$$\tilde{F}_t(s,s') \stackrel{\text{def}}{=} \neg Ds_t(s) \wedge \bigwedge_{p_i\in t\bullet} (m'_i \wedge x'_i = 0) \wedge \bigwedge_{p_i\in \bullet t\setminus t\bullet} (\neg m'_i \wedge x'_i = 0)$$
$$\vee \bigwedge_{p_i\in(\bullet t\cup t\bullet)} (m'_i \leftrightarrow m_i \wedge x'_i = x_i)$$

したがって，1 ステップを表す削減された論理式 $\tilde{\mathcal{T}}$ は以下となる．

$$\tilde{\mathcal{T}}(s,s') \stackrel{def}{=} \tilde{C}(s,s'') \wedge \tilde{F}_t(s'',s')$$

■提案表現の変数削減　同様に $\mathcal{C}^{DL}$，F_t^{DL} からそれぞれ共通する部分論理式を括り出す．

$$\mathcal{C}^{DL}(s,s') \stackrel{\text{def}}{=} \left(\bigwedge_{t\in T} \neg En_t^{DL}(s) \wedge (c' - c > 0) \vee (c' - c = 0)\right) \bigwedge_{p_i\in P} (z'_i = z_i \wedge m'_i \leftrightarrow m_i)$$

$$F_t^{DL}(s,s') \stackrel{\text{def}}{=} \Bigg(\bigwedge_{t\in T} \neg Ds_t^{DL}(s) \wedge \bigwedge_{p_i\in\bullet t} (m'_i \wedge z'_i = c) \wedge \bigwedge_{p_i\in\bullet t\setminus t\bullet} (\neg m'_i \wedge z'_i = z_i)$$
$$\vee \bigwedge_{\bullet t\cup t\bullet} (m'_i \leftrightarrow m_i \wedge z'_i = z_i)\Bigg) \wedge \bigwedge_{p_i\in P\setminus(\bullet t\cup t\bullet)} (m'_i \leftrightarrow m_i \wedge z'_i = z_i) \wedge (c' - c = 0)$$

よって，Algorithm2 に示すアルゴリズムに従って共通部分を削除して変数の置き換えを行うことで以下の論理式に削減される．

$$\tilde{\mathcal{C}}^{DL}(s,s') \stackrel{\text{def}}{=} \bigwedge_{t\in T} \neg En_t^{DL}(s) \wedge (c' - c > 0) \vee (c' - c = 0)$$

$$\tilde{F}_t^{DL}(s,s') \stackrel{\text{def}}{=} \bigwedge_{t\in T} \neg Ds_t^{DL}(s) \wedge \bigwedge_{p_i\in\bullet t} (m'_i \wedge z'_i = c) \wedge \bigwedge_{p_i\in\bullet t\setminus t\bullet} (\neg m'_i \wedge z'_i = z_i)$$
$$\vee \bigwedge_{\bullet t\cup t\bullet} (m'_i \leftrightarrow m_i \wedge z'_i = z_i)$$

したがって，1 ステップを表す削減された論理式 $\tilde{T}^{DL}$ は以下となる．

$$\tilde{\mathcal{T}}^{DL}(s,s') \stackrel{def}{=} \tilde{\mathcal{C}}^{DL}(s,s'') \wedge \tilde{F}_t^{DL}(s'',s')$$

Algorithm 1 従来表現の変数削減

1: **for** $p_i \in P$ **do**{
2: $e_i := 0$;
}
3: $j := 0$;
4: $Y := I(s)|_{s_i \to s_{i,0}\ \texttt{for all}\ p_i \in P}$;
5: **for** $step = 1, \cdots, k$ **do**{
6: $j := j + 1$;
7: $Y := Y \wedge \bigwedge_{t \in T} \neg En_t(s_{i,e_i})$
8: $\wedge \bigwedge_{p_i \in P}(x_{i,j} = x_{i,e_i} + d) \wedge d_{step} > 0 \vee \bigwedge_{p_i \in P}(x_{i,j} = x_{i,e_i}) \wedge d_{step} = 0$
9: **for** 時間経過で変化する変数 v_i **do**{
10: $e_i := j$
}
11: **for** $t \in T$ **do**{
12: $j := j + 1$
13: $Y := Y \wedge \neg Ds_t(s_{i,e_i}) \wedge \bigwedge_{p_i \in t\bullet}(m_{i,j} \wedge x_{i,j} = 0) \wedge \bigwedge_{p_i \in \bullet t \setminus t\bullet}(\neg m_{i,j} \wedge x_{i,j} = 0)$
14: $\vee \bigwedge_{p_i \in (\bullet t \cup t\bullet)}(m_{i,j} \leftrightarrow m_{i,e_i} \wedge x_{i,j} = x_i)$
15: **for** トランジション t の発火で変化する変数 v_i **do**{
16: $e_i := j$
}
}
}

Algorithm 2 提案表現の変数削減

for $p_i \in P$ **do**{
    $e_i := 0$;
}
$j := 0$;
$Y := I(s)|_{s_i \to s_{i,0}\ \texttt{for all}\ p_i \in P}$;
for $step = 1, \cdots, k$ **do**{
    $j := j + 1$;
    $Y := Y \wedge \bigwedge_{t \in T} \neg En_t^{DL}(s_{i,e_i}) \wedge (c_j - c_{e_i} > 0) \vee (c_j - c_{e_i} = 0)$
    for 時間経過で変化する変数 v_i **do**{
        $e_i := j$
    }
    for $t \in T$ **do**{
        $j := j + 1$
        $Y := Y \wedge \bigwedge_{t \in T} \neg Ds_t^{DL}(s_{i,e_i}) \wedge \bigwedge_{p_i \in {}^\bullet t}(m_{i,j} \wedge z_{i,j} = c_{e_i}) \wedge$
        $\bigwedge_{p_i \in {}^\bullet t \setminus t^\bullet}(\neg m_{i,j} \wedge z_{i,j} = z_{i,e_i})$
        $\vee \bigwedge_{{}^\bullet t \cup t^\bullet}(m_{i,j} \leftrightarrow m_{i,e_i} \wedge z_{i,j} = z_{i,e_i})$
        for トランジション t の発火で変化する変数 v_i **do**{
            $e_i := j$
        }
    }
}

6.3 補間に基づく非有界モデル検査の適用

k ステップ以内に特性を満たす状態に到達することを表す論理式を $BMC_k \stackrel{\text{def}}{=} \mathcal{N}_k \wedge \mathcal{R}_k$ とおく．そして，BMC_k を $BMC_k = PREF \wedge SUFF^k$ となるように以下の 2 つの部分論理式 $PREF$ および $SUFF^k$ へと分割する．

$$\begin{aligned} PREF =& \mathcal{I}(s_0) \wedge \mathcal{T}(s_0, s_n) \\ SUFF^k =& \bigwedge_{1 \le i \le k} \mathcal{T}(s_{i*n}, s_{i(n+1)}) \wedge R(s_{k*(n+1)}) \end{aligned}$$

このとき，$PREF \wedge SUFF^k$ が充足可能ならば性質を満たす状態 s_{k*n} に到達可能である．充足不能であれば，$PREF$ と $SUFF^k$ から SMT ソルバは補間論理式 $Inter$ を生成する．5.4 節で述べた補間の条件 (3) から $Inter$ は s_n に関する論理式である．したがって，条件 (2) より，$Inter$ は初期状態から 1 ステップで到達可能なすべての状態を含む集合，すなわち初期状態から 1 ステップで到達可能な状態の上方近似集合となる．この $Inter$ を初期状態の特性関数 $\mathcal{I}$ と置き換えて新たに

$$PREF = Inter(s_0) \wedge \mathcal{T}(s_0, s_{n+1})$$

として再び充足可能性判定を行う．充足不能であれば，得られた補間論理式 $Inter'$ を再び初期状態として充足可能性判定を行う．初期状態を $Inter$ で更新する度に，状態集合は現在の状態から 1 ステップで到達可能な状態集合の上方近似に置き換えられるので，この処理を $Inter' = Inter$ となるまで繰り返すことで，$Inter$ は初期状態から到達可能なすべての状態集合の上方近似となる．この $Inter$ を初期状態として SMT ソルバによる充足可能性判定を行った結果が充足不能であれば，求める状態へは到達不能との結論が得られる．

一方，途中で充足可能という結果が得られた場合，$Inter$ は到達可能状態の上方近似であるため，得られた割り当てが偽反例である可能性がある．このときはステップ数 k を延長した上で再度 BMC_k の充足可能性判定を行う．状態空間は有限なので，いつかこの手続きは終了する．

第 7 章

検証コストの評価

7.1 実験環境

評価のため，提案表現と従来表現と比較した．本実験は Ubuntu 16.04 LTS OS，Intel Core i7 7700 3.6 GHz CPU，64 GB メモリ を用いて実施した．SMT ソルバには SMT-COMP 2018 [48] で上位 5 つの MathSAT [49]，Z3 [50]，SMTInterpol [51]，yices [52]，CVC4 [53] を用いた．SMT ソルバの実行時に従来表現が線形制約上の論理として扱われるように，SMT ソルバのオプションとして (set-logic:QF_UFLIA) を指定し，提案表現が差分論理上の論理として扱われるように (set-logic:QF_UFIDL) を指定した．

また，同様の計算機環境で T-TPN に対する有界モデル検査の検証コストを評価した．SMT ソルバは yices を用いた．

そして Mac OS X 10.10.5 OS，Intel Core i5 2.6GHz CPU，16GB メモリ を用いて，非有界モデル検査を評価した．SMT ソルバは補間をサポートしている MathSAT を用いた．いずれの評価においても検査特性はデッドロック検出とした．

7.2 検査対象となる時間ペトリネット

P-TPN の従来表現と提案表現を用いた有界モデル検査の評価には表 7.1 に示す P-TPN を対象とした．これらは非同期回路をモデル化した P-TPN であり，safe P-TPN であることが既知である．

T-TPN の有界モデル検査で用いる T-TPN を表 7.2 と表 7.3 に示す．表 7.2 の T-TPN は車の交通の流れをモデル化した safe ではない T-TPN であり，デッドロックをもつ．すなわち，各プレイスが 2 つ以上のトークンをもつことが許される T-TPN である．

表 7.1　有界モデル検査の対象とした safe P-TPN

P-TPN	プレイス	トランジション
#1	374	389
#2	1030	1193
#3	3206	4049

表 7.2　有界モデル検査の対象とした T-TPN

プレイス数	トランジション数
28	52

表 7.3　有界モデル検査の対象とした safe T-TPN

T-TPN	プレイス数	トランジション数
m1	735	570
m2	1119	874
m3	2127	1674

表 7.4　非有界モデル検査の対象とした safe P-TPN

プレイス数	トランジション数
26	18

表 7.3 の T-TPN は通信プロトコルをモデル化した safe T-TPN であり，デッドロックをもつ．ここで T-TPN が safe の場合であっても 6.1.2 と同様の枠組みで有界モデル検査を適用することができる．

P-TPN の非有界モデル検査で用いたで P-TPN を表 7.4 に示す．これは表 7.1 に示した P-TPN と同様に非同期回路をモデル化した P-TPN であり，デッドロックフリーであることが既知である．

7.3 有界モデル検査における検証コスト

7.3.1 P-TPN の検証

表 7.5 は，変数削減による論理式のサイズ削減の効果の比較を示している．“変数” は論理式内で宣言された変数を表し，“制約” は論理式内の論理的制約を表す．ここで論理的制約は，ブール変数 x，y に対する x，$\neg x$，$x \leftrightarrow y$ および線形制約上の制約を表す．表 7.5 に示すように，変数と制約の数は変数の置換によって著しく削減され，削減は従来表現に比して提案表現に対してより良く機能している．

表 7.5　変数削減の効果

		変数				制約			
	ステップ	削減後		削減前		削減後		削減前	
		LA	DL	LA	DL	LA	DL	LA	DL
	1	292,469	292,859	3,815	3,442	12,016	10,908	300,670	300,325
	2	584,190	584,969	6,882	6,135	20,887	19,031	598,195	597,865
	3	875,911	877,079	9,949	8,828	29,758	27,154	895,720	895,405
	4	1,167,632	1,169,189	13,016	11,521	38,629	35,277	1,193,245	1,192,945
#1	5	1,459,353	1,461,299	16,083	14,214	47,500	43,400	1,490,770	1,490,485
	6	1,751,074	1,753,409	19,150	16,907	56,371	51,523	1,788,295	1,788,025
	7	2,042,795	2,045,519	22,217	19,600	65,242	59,646	2,085,820	2,085,565
	8	2,334,516	2,337,629	25,284	22,293	74,113	67,769	2,383,345	2,383,105
	9	2,626,237	2,629,739	28,351	24,986	82,984	75,892	2,680,870	2,680,645
	10	2,917,958	2,921,849	31,418	27,679	91,855	84,015	2,978,395	2,978,185
	1	2,461,701	2,462,895	11,479	10,450	36,703	33,639	2,486,925	2,486,084
	2	4,921,342	4,923,729	20,898	18,839	64,131	59,007	4,964,575	4,963,897
	3	7,380,983	7,384,563	30,317	27,228	91,559	84,375	7,442,225	7,441,710
	4	9,840,624	9,845,397	39,736	35,617	118,987	109,743	9,919,875	9,919,523
#2	5	12,300,265	12,306,231	49,155	44,006	146,415	135,111	12,397,525	12,397,336
	6	14,759,906	14,767,065	58,574	52,395	173,843	160,479	14,875,175	14,875,149
	7	17,219,547	17,227,899	67,993	60,784	201,271	185,847	17,352,825	17,352,962
	8	19,679,188	19,688,733	77,412	69,173	228,699	211,215	19,830,475	19,830,775
	9	22,138,829	22,149,567	86,831	77,562	256,127	236,583	22,308,125	22,308,588
	10	24,598,470	24,610,401	96,250	85,951	283,555	261,951	24,785,775	24,786,401
	1	25,975,013	25,979,063	38,423	35,218	123,766	114,198	26,060,356	26,058,043
	2	51,943,614	51,951,713	70,434	64,023	217,152	201,172	52,090,332	52,088,862
	3	77,912,215	77,924,363	102,445	92,828	310,538	288,146	78,120,308	78,119,681
	4	103,880,816	103,897,013	134,456	121,633	403,924	375,120	104,150,284	104,150,500
#3	5	129,849,417	129,869,663	166,467	150,438	497,310	462,094	130,180,260	130,181,319
	6	155,818,018	155,842,313	198,478	179,243	590,696	549,068	156,210,236	156,212,138
	7	181,786,619	181,814,963	230,489	208,048	684,082	636,042	182,240,212	182,242,957
	8	207,755,220	207,787,613	262,500	236,853	777,468	723,016	208,270,188	208,273,776
	9	233,723,821	233,760,263	294,511	265,658	870,854	809,990	234,300,164	234,304,595
	10	259,692,422	259,732,913	326,522	294,463	964,240	896,964	260,330,140	260,335,414

表 7.6 は 3 つの TPN に対する 1 から 10 ステップまでの 有界モデル検査の実行時間を示している．“LA” と “DL” の列はそれぞれ従来表現と提案表現の実行時間を表す．タイムアウトは 600 秒に設定した．“結果” の列に示すように，デッドロックは 10 ステップ以内では検出されなかった．すべての SMT ソルバについて，提案表現は従来表現より良い結果を示した．特に yices は，対象の TPN の規模が大きくなったとしても，DL での論理式に対して良い結果を示した．いくつかの場合では，LA での論理式に対して DL での論理式より良い結果となった．論理式のサイズはあまり大きくないため，論理式の構造の差異が，高速なアルゴリズムの効果よりも実行時間に影響したようである．

表 7.6　P-TPN に対する有界モデル検査の実行時間の比較 (sec.)

	ステップ	MathSAT		Z3		SMTIinterpol		yices		CVC4		結果
		LA	DL	LA	DL	LA	DL	LA	DL	LA	DL	
	1	0.043	0.031	0.031	0.031	0.479	0.420	0.012	0.015	0.149	0.148	unsat
	2	0.069	0.061	0.071	0.071	0.629	0.570	0.023	0.027	0.277	0.270	unsat
	3	0.118	0.116	0.138	0.137	0.730	0.690	0.035	0.041	0.421	0.405	unsat
	4	0.219	0.186	0.250	0.238	0.941	0.891	0.048	0.057	0.544	0.524	unsat
#1	5	4.182	1.097	0.965	0.785	6.158	8.586	6.397	0.209	1.113	1.008	unsat
	6	5.325	2.876	2.989	1.813	11.633	11.916	16.283	0.544	2.860	1.406	unsat
	7	18.612	3.956	8.524	3.264	17.235	39.502	12.725	0.590	3.395	2.454	unsat
	8	19.148	10.185	14.632	5.260	78.673	58.682	14.222	1.393	11.403	4.746	unsat
	9	31.172	17.919	33.772	11.692	201.717	187.003	32.164	3.885	49.292	14.752	unsat
	10	78.780	42.962	61.003	32.251	> 600	258.586	91.310	7.780	69.900	184.923	unsat
	1	0.103	0.108	0.107	0.104	0.888	0.843	0.038	0.046	0.620	0.549	unsat
	2	0.353	0.283	0.384	0.333	2.880	1.499	0.089	0.101	1.304	1.143	unsat
	3	0.878	0.557	1.040	0.717	2.187	2.130	0.343	0.173	1.987	1.754	unsat
	4	1.799	1.082	1.775	1.343	10.130	6.396	0.854	0.291	2.762	2.418	unsat
#2	5	6.991	4.115	4.165	4.024	16.678	35.643	4.230	0.427	3.969	3.582	unsat
	6	10.310	6.721	8.226	6.014	55.335	62.101	9.524	1.229	11.929	5.239	unsat
	7	40.479	46.537	29.248	14.886	148.538	294.035	42.590	4.308	20.572	10.864	unsat
	8	65.158	68.318	77.255	37.106	591.304	320.213	71.035	8.127	65.388	29.093	unsat
	9	88.706	53.858	118.414	84.530	> 600	> 600	212.159	19.547	208.174	73.094	unsat
	10	296.510	173.050	224.211	135.838	—	—	340.504	48.888	389.901	204.180	unsat
	1	0.371	0.384	0.437	0.415	1.867	1.775	0.129	0.160	1.837	1.827	unsat
	2	1.727	1.520	2.706	1.715	10.087	10.064	0.468	0.460	4.804	4.819	unsat
	3	5.398	3.688	7.790	4.658	23.477	19.291	2.835	1.011	7.868	7.157	unsat
	4	11.624	7.474	16.579	9.238	130.407	104.760	26.152	2.488	10.562	9.784	unsat
#3	5	49.279	21.836	63.565	25.299	91.997	215.889	89.636	5.140	14.849	13.539	unsat
	6	173.166	89.663	156.303	96.474	> 600	> 600	150.506	16.581	31.128	28.166	unsat
	7	335.292	337.237	> 600	188.084	—	—	> 600	32.838	304.836	81.453	unsat
	8	> 600	> 600	—	> 600	—	—	—	139.254	451.156	404.832	unsat
	9	—	—	—	—	—	—	—	240.595	> 600	> 600	unsat
	10	—	—	—	—	—	—	—	> 600	—	—	N/A

表 7.7　T-TPN に対する変数削減効果

ステップ数	変数		制約	
	削減後	削減前	削減後	削減前
1	1,220	4,374	38,165	41,319
2	2,359	8,667	75,533	81,841
3	3,498	12,960	112,901	122,363
4	4,637	17,253	150,269	162,885
5	5,776	21,546	187,637	203,407
6	6,915	25,839	225,005	243,929
7	8,054	30,132	262,373	284,451
8	9,193	34,425	299,741	324,973
9	10,332	38,718	337,109	365,495
10	11,471	43,011	374,477	406,017
11	12,610	47,304	411,845	446,539
12	13,749	51,597	449,213	487,061
13	14,888	55,890	486,581	527,583
14	16,027	60,183	523,949	568,105
15	17,166	64,476	561,317	608,627
16	18,305	68,769	598,685	649,149
17	19,444	73,062	636,053	689,671
18	20,583	77,355	673,421	730,193
19	21,722	81,648	710,789	770,715
20	22,861	85,941	748,157	811,237

7.3.2　T-TPN の検証

表 7.7 は，変数削減による論理式のサイズ削減の効果を示している．表 7.5 と同様，表 7.7 に示すように変数と制約の数は変数の置換によって著しく削減されている．

表 7.8　T-TPN に対する有界モデル検査の実行時間

ステップ	実行時間 (sec.)	結果
1	0.040	unsat
2	0.164	unsat
3	0.483	unsat
4	1.331	unsat
5	4.107	unsat
6	10.422	unsat
7	30.119	unsat
8	106.142	unsat
9	433.035	unsat
10	2356.413	unsat
11	11476.475	unsat
12	45718.161	unsat
13	927.804	sat
14	879.981	sat
15	519.758	sat
16	545.453	sat
17	765.037	sat
18	425.540	sat
19	223.980	sat
20	298.186	sat

表 7.8 に表 7.2 に示した T-TPN に対して有界モデル検査を実行した結果を示す．表 7.8 は 1 から 20 ステップまでの 有界モデル検査の実行時間を示している．“結果” の列に示すように，デッドロックは 13 ステップで検出された．デッドロックが検出されるまでの 12 ステップまではステップが増加するごとに実行時間が増加しているが，デッドロックが検出されてからの 13 ステップ以降の実行時間は，それまでの実行時間より小さい傾向にある．これは，各ステップで表現された状態空間のすべてを充足可能性判定によって探索し終える前にデッドロックを検出したためと考えられる．

続いて，表 7.3 に示す T-TPN を対象に，P-TPN の論理式表現との有界モデル検査の実行時間を比較する．P-TPN の論理式表現は提案表現を用いる．表 7.3 の T-TPN は safe T-TPN であり，safe P-TPN への等価な変換が可能である．

表 7.3 の T-TPN に対する有界モデル検査の実行時間を表 7.9，7.10，7.11 にそれぞれ示す．タイムアウトは 600 秒に設定し，ステップ数は 1 から 20 ステップまでとした．各表より，すべての結果においてデッドロックは検出されなかった．表 7.9 と表 7.10 では，T-TPN の論理式表現が提案表現より短いステップでタイムアウトが発生し，表 7.11 では提案表現が T-TPN の論理式表現より短いステップでタイムアウトが発生した．また表 7.11 においては，結果が得られたステップでの実行時間について，全体として高速に終了している傾向にある．

表 7.9　safe T-TPN に対する有界モデル検査の実行時間 (m1)

ステップ	P-TPN（提案表現）		T-TPN	
	実行時間 (sec.)	結果	実行時間 (sec.)	結果
1	0.047	unsat	0.073	unsat
2	0.113	unsat	0.150	unsat
3	0.201	unsat	0.240	unsat
4	0.295	unsat	0.346	unsat
5	0.616	unsat	0.446	unsat
6	1.033	unsat	0.620	unsat
7	1.690	unsat	1.392	unsat
8	2.735	unsat	1.755	unsat
9	8.323	unsat	19.501	unsat
10	12.881	unsat	23.790	unsat
11	48.358	unsat	149.268	unsat
12	23.182	unsat	> 600	N/A
13	103.071	unsat	—	—
14	299.132	unsat	—	—
15	> 600	N/A	—	—
16	—	—	—	—
17	—	—	—	—
18	—	—	—	—
19	—	—	—	—
20	—	—	—	—

表 7.10　safe T-TPN に対する有界モデル検査の実行時間 (m2)

ステップ	P-TPN（提案表現）		T-TPN	
	実行時間 (sec.)	結果	実行時間 (sec.)	結果
1	0.077	unsat	0.105	unsat
2	0.185	unsat	0.247	unsat
3	0.312	unsat	0.400	unsat
4	0.678	unsat	0.559	unsat
5	0.914	unsat	0.706	unsat
6	1.771	unsat	0.850	unsat
7	2.358	unsat	1.029	unsat
8	4.512	unsat	1.221	unsat
9	8.394	unsat	1.589	unsat
10	16.843	unsat	6.143	unsat
11	25.310	unsat	15.230	unsat
12	153.203	unsat	29.370	unsat
13	96.641	unsat	158.500	unsat
14	98.096	unsat	> 600	N/A
15	456.513	unsat	—	—
16	> 600	N/A	—	—
17	—	—	—	—
18	—	—	—	—
19	—	—	—	—
20	—	—	—	—

表 7.11　safe T-TPN に対する有界モデル検査の実行時間 (m3)

ステップ	P-TPN（提案表現）		T-TPN	
	実行時間 (sec.)	結果	実行時間 (sec.)	結果
1	0.158	unsat	0.237	unsat
2	0.388	unsat	0.546	unsat
3	0.681	unsat	0.859	unsat
4	1.193	unsat	1.190	unsat
5	1.578	unsat	1.519	unsat
6	3.393	unsat	1.822	unsat
7	4.749	unsat	2.231	unsat
8	6.017	unsat	2.525	unsat
9	17.303	unsat	2.892	unsat
10	23.437	unsat	3.218	unsat
11	64.398	unsat	3.548	unsat
12	72.155	unsat	3.868	unsat
13	157.773	unsat	4.258	unsat
14	211.452	unsat	6.151	unsat
15	322.584	unsat	15.220	unsat
16	538.693	unsat	190.186	unsat
17	> 600	N/A	457.124	unsat
18	—	—	> 600	N/A
19	—	—	—	—
20	—	—	—	—

7.4 非有界モデル検査における検証コスト

次に，表 7.4 に示した P-TPN に対する非有界モデル検査についての実験結果を示す．従来表現と提案表現で論理式を作成し，MathSAT を用いて非有界モデル検査を行った結果を図 7.12 に示す．グラフの横軸 $i(j)$ は，i ステップを表す論理式に対して補間論理式を j 回求めた時点での充足可能性判定であることを表しており，縦軸は判定に要した時間を表している．また，縦軸の値はその時点での累積の処理時間となっている．

図 7.12 より，従来表現と提案表現の双方で非有界モデル検査のアルゴリズムが終了し，デッドロックフリーであることを検出した．実行時間については提案手法でかつ変数削減を適用した場合が最も良く，変数削減の効果が強く表れる結果となった．この場合，ステップ数 6 で補間生成回数 4 の時点でアルゴリズムが終了した．最も時間を要した従来表現に変数削減を適用しない場合は，ステップ数 6 で補間論理式生成回数 2 の時点でアルゴリズムが終了している．

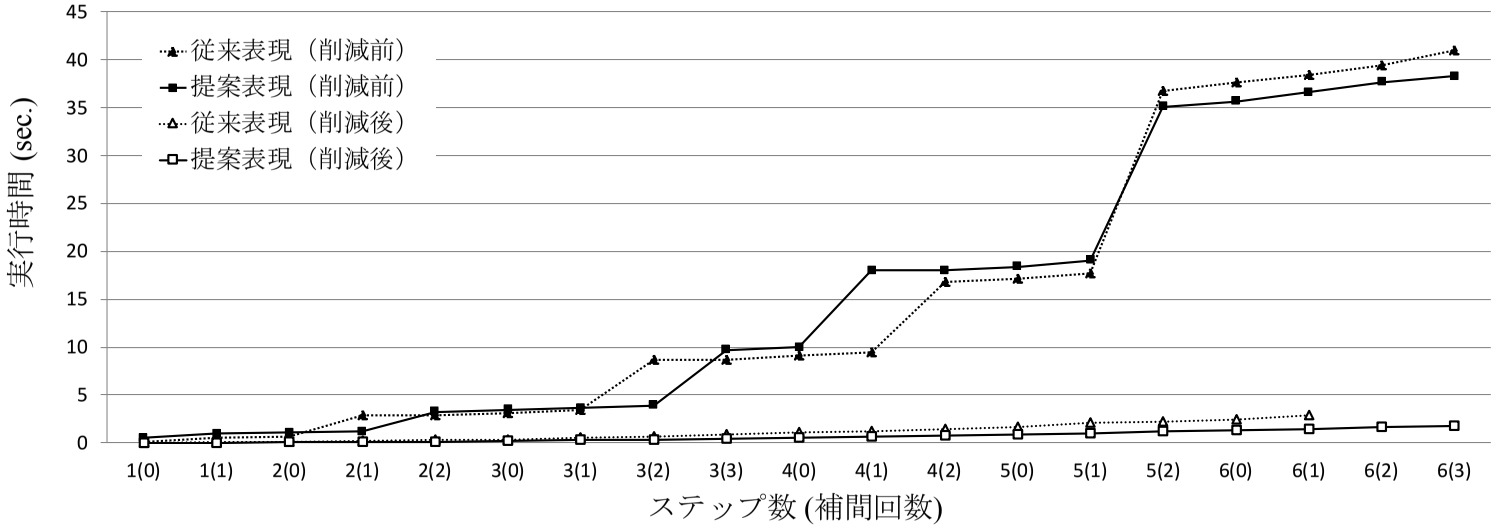


表 7.12　非有界モデル検査の実行時間

第 8 章

まとめ

本論文では，モデル検査を用いた心拍モニタリングに基づく心拍モニタリングに基づく車体制御システムの高信頼化を目的として，UWB センサを用いた非接触心拍モニタリング手法と時間ペトリネットの効率的な有界モデル検査手法を提案した．

初めに，車内における非接触による心拍検出の実現を目的として MIMO レーダーおよび UWB センサによる非接触な RRI 検出の実現について述べた．接触型心拍計測機器の myBeat を比較対象として MIMO レーダ，UWB センサ，myBeat を被験者および車内に設置して RRI の検出実験を実施した．実験から得られた各機器の RRI をもとに Bland-Altman プロットをそれぞれ作成し，算出された誤差範囲 (LOA) を比較した．結果として，UWB センサから得られた RRI が MIMO レーダから得られた RRI より myBeat の RRI に近いことが明らかとなり，UWB センサによる心拍検出が MIMO レーダに比べ精度が高いことが示された．最後に UWB センサと myBeat から得られた RRI を用いて LF/HF をそれぞれ算出し，それらを比較した結果， UWB センサの RRI の測定精度が myBeat の RRI の測定精度に対して十分高いことが示された．

次に，心拍モニタリングに基づく車体制御システムに要求される厳格な時間制約を満たされているかを保証するため，リアルタイムシステムのモデル化に用いられる時間ペトリネットを対象とした有界モデル検査の効率化手法について述べた．

時間ペトリネットの振る舞いを表す論理式内の線形制約を差分論理によって表現することで，高速な充足可能性判定アルゴリズムを適用可能にした．従来の線形制約による論理式表現を比較対象に，提案した論理式表現と有界モデル検査の実行時間を比較することで提案する論理式表現の有効性を示した．よって，時間ペトリネットでモデル化された車体制御システムに対して差分論理表現による有界モデル検査を適用することで，大規模な状態をもつ車体制御システムを効率的に検証するための見通しを得た．

また，他のクラスに属している時間ペトリネットの論理式表現を提案することで，より一般的な時間ペトリネットの振る舞いを対象とした有界モデル検査を実現した．さらに安全性検証を可能にするため，時間ペトリネットの非有界モデル検査手法を提案した．

今後の方針として，心拍モニタリングシステムに関しては非接触での呼吸の検出が挙げられる．呼吸の変化は体調の変化を表すため，呼吸をモニタリングすることで不調の検出に利用することができる [12, 54]．また，RRI から異常を検出することも重要な課題である．実験では正常な RRI を計測することを目的としたが，異常時は正常な RRI は得られない．このときの異常の検出方法を検討する必要がある．さらにセンシングの精度向上も求められる．例えば，加速度センサや画像センサを組み合わせて多角的に対象者を捉えることによる精度向上が挙げられる．これらのセンサを用いて対象者の体動等を検出することで，それらをノイズとして除去することができる．車体制御システムの妥当性検証については，車体制御システムをモデル化した時間ペトリネットを用いた有界モデル検査の適用とその評価が今後の課題として挙げられる．その際，車体制御システムを時間ペトリネットへモデル化する手法も検討する必要がある．

謝辞

岡山県立大学情報工学部の横川智教准教授には，学士の課程より博士課程に至るまでの 7 年間に渡って直接ご指導賜りました．その的確な助言と懇篤なるご配慮を以って研究活動全体を支えて頂き，学術研究の基礎をご示唆くださりましたことには感謝の念に堪えません．重ねて心より感謝申し上げます．

本研究の終始に渡ってご配慮頂き，また補助研究員としての活動を通して様々なご支援賜りました岡山県立大学情報工学部の有本和民教授に深謝いたします．

本論文の基礎となる論文の共著者である川崎医療福祉大学の茅野功教授には，論文採択に至るまでに多大なるご助力を頂きました．ここに感謝申し上げます．また同論文の核となる部分は，もう一人の共著者である岡山県立大学情報工学部情報システム工学科を卒業した藤井健斗君が先駆けとなって礎を築いてくださいました．本当に有り難う御座います．

私の学位取得に対し，折りあるごとにご高配賜りました岡山県立大学情報工学部の渡辺富夫教授，石井裕准教授，佐藤洋一郎教授に深く感謝いたします．

本論文を副査として御審査頂きました岡山県立大学情報工学部の尾崎公一教授，並びに大阪大学大学院情報科学研究科の土屋達弘教授に感謝いたします．

岡山県立大学附属図書館のアルバイトでの経験は，研究では培うことのできない視座が養われ，研究を俯瞰して捉える視野を与えて頂きました．この貴重な経験は今後の私の人生においても大きな財産となることと思います．直接ご指導頂きました田中智子図書館司書に心からの感謝を申し上げます．

最後に，私の進路を案じながらも博士課程に進学することを許し，支えてくれた両親と兄姉に衷心より感謝申し上げます．

参考文献

[1] SAE international, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," https://www.sae.org/standards/content/j3016_201806, 2018.

[2] K. Bengler, K. Dietmayer, B. Farber, M. Maurer, C. Stiller, and H. Winner, "Three decades of driver assistance systems: Review and future perspectives," *IEEE Intelligent Transportation Systems Magazine*, vol. 6, no. 4, pp. 6–22, 2014.

[3] M. Ramzan, H. U. Khan, S. M. Awan, A. Ismail, M. Ilyas, and A. Mahmood, "A survey on state-of-the-art drowsiness detection techniques," *IEEE Access*, vol. 7, pp. 61 904–61 919, 2019.

[4] S.-Y. Hsu, Y.-L. Chen, P.-Y. Chang, J.-Y. Yu, T.-F. Yang, R.-J. Chen, and C.-Y. Lee, "A Micropower Biomedical Signal Processor for Mobile Healthcare Applications," in *Proc. of IEEE Asian Solid-State Circuits Conference (ASSCC)*, 2011, pp. 301–304.

[5] Y. Zhang, M. Berthelot, and B. Lo, "Wireless Wearable Photoplethysmography Sensors for Continuous Blood Pressure Monitoring," in *Proc. of the Annual IEEE Wireless Health Conference 2016*, 2016, pp. 81–88.

[6] Y. Tanaka, S. Izumi, Y. Kawamoto, H. Kawaguchi, and M. Yoshimoto, "Adaptive Noise Cancellation Method for Capacitively Coupled ECG Sensor using Single Insulated Electrode," in *Proc. of 2016 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, 2016, pp. 296–299.

[7] K. J. Lee, C. Park, and B. Lee, "Tracking driver's heart rate by continuous-wave Doppler radar," in *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2016, pp. 5417–5420.

[8] L. Ren, Y. S. Koo, H. Wang, Y. Wang, Q. Liu, and A. E. Fathy, "Noncontact

multiple heartbeats detection and subject localization using uwb impulse doppler radar," *IEEE Microwave and Wireless Components Letters*, vol. 25, no. 10, pp. 690–692, Oct. 2015.

[9] L. Ren, H. Wang, K. Naishadham, O. Kilic, and A. E. Fathy, "Phase-based methods for heart rate detection using uwb impulse doppler radar," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 10, pp. 3319–3331, 2016.

[10] K. Shyu, L. Chiu, P. Lee, T. Tung, and S. Yang, "Detection of breathing and heart rates in uwb radar sensor data using fvpief-based two-layer eemd," *IEEE Sensors Journal*, vol. 19, no. 2, pp. 774–784, Jan. 2019.

[11] T. Sakamoto, R. Imasaka, H. Taki, T. Sato, M. Yoshioka, K. Inoue, T. Fukuda, and H. Sakai, "Feature-based correlation and topological similarity for interbeat interval estimation using ultrawideband radar," *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 4, pp. 747–757, Apr. 2016.

[12] A. Al-Naji, K. Gibson, S. Lee, and J. Chahl, "Monitoring of cardiorespiratory signal: Principles of remote measurements and review of methods," *IEEE Access*, vol. 5, pp. 15 776–15 790, 2017.

[13] K. Konishi, and T. Sakamoto, "Automatic tracking of human body using millimeter-wave adaptive array radar for noncontact heart rate measurement," in *2018 Asia-Pacific Microwave Conference (APMC)*, Nov. 2018, pp. 836–838.

[14] Q. Deng, J. Le, S. Barbat, R. Tian, and Y. Chen, "Efficient living subject localization and weak vital-sign signal enhancement using impulse radio based uwb radar," in *2019 IEEE Intelligent Vehicles Symposium (IV)*, June 2019, pp. 777–782.

[15] J. Li, and P. Stoica, *MIMO Radar Signal Processing*. John Wiley & Sons, Ltd, 2008.

[16] Z.Peng, and C.Li, "Portable microwave radar systems for short-range localization and life tracking: A review," *Sensors*, vol. 19, no. 5, p. 1136, Mar. 2019.

[17] H. Ajorloo, C. Sreenan, A. Loch, and J. Widmer, "On the feasibility of using ieee 802.11ad mmwave for accurate object detection," in *Proc. of the 34th ACM/SIGAPP Symposium on Applied Computing*, Apr. 2019, pp. 2406–2413.

[18] 渡辺 恭，阪本 卓也，今西 亮介，奥村 成皓，佐藤 亨，吉岡 元貴，井上 謙一，福田 健志，酒井 啓之，"B-20-18 超広帯域 MIMO アレイレーダによる夜間睡眠中の心拍高精度推定 (B-20. ヘルスケア・医療情報通信技術, 一般セッション)"，電子情報通信学

会総合大会講演論文集，vol. 2016，no. 1，p. 665，Mar. 2016.

[19] Q. Liu, H. Guo, J. Xu, H. Wang, A. Kageza, S. AlQarni, and S. Wu, "Non-contact non-invasive heart and respiration rates monitoring with mimo radar sensing," in *2018 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2018, pp. 1–6.

[20] K. Arimoto, D. Yamashita, N. Igawa, T. Yokogawa, Y. Sato, I. Kayano, and A. Shiratori, "A Smart low power R-R-I heartbeat monitor system with contactless UWB sensor," in *14th International SoC Design Conference (ISOCC 2017) ET2-4*, 2017, pp. 63–64.

[21] N. Igawa, T. Yokogawa, K. Fujii, I. Kayano, Y. Sato, and K. Arimoto, "An in-vehicle contact-less heartbeat monitoring system using uwb sensor," *IEEJ Transactions on Sensors and Micromachines*, vol. 139, no. 10, pp. 366–367, 2019.

[22] J. M. Bland, and D. Altman, "Statistical methods for assessing agreement between two methods of clinical measurement," *The Lancet*, vol. 327, no. 8476, pp. 307 – 310, 1986.

[23] M. Malik, "Heart rate variability: Standards of measurement, physiological interpretation, and clinical use," *Circulation*, vol. 93, pp. 1043–1065, Mar. 1996.

[24] P. Merlin, and D. Farber, "Recoverability of Communication Protocols–Implications of a Theoretical Study," *IEEE Trans. Comm.*, vol. 24, no. 9, pp. 1036–1043, Sep. 1976.

[25] Berthomieu B，Ribet P，Vernadat F，"The tool TINA - Construction of abstract state spaces for Petri nets and Time Petri nets"，International Journal of Production Research，vol. 42，no. 14，pp. 2741–2756，2004.

[26] D. Lime, O. H. Roux, C. Seidner, and L. M. Traonouez, "Romeo: A parametric model-checker for petri nets with stopwatches," in *Proc. of 15th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2009)*, vol. 5505 LNCS, 2009, pp. 54–57.

[27] A. Biere, A. Cimatti, E. M. Clarke, and Y. Zhu, "Symbolic Model Checking without BDDs," in *Proc. of the 5th Int'l Conf. on Tools and Algorithms for Construction and Analysis of Syst. (TACAS '99)*, 1999, pp. 193–207.

[28] G. Audemard, A. Cimatti, A. Kornilowicz, and R. Sebastiani, "SAT-Based bounded model checking for timed systems," in *Proc. of the 22nd IFIP WG 6.1 Int'l Conf. Houston on Formal Tech. for Networked and Distributed Syst.*

(FORTE 2002), 2002, pp. 243–259.

[29] M. Sorea, "Bounded Model Checking for Timed Automata," *Electron. Notes Theor. Comput. Sci.*, vol. 68, no. 5, pp. 116–134, May 2003.

[30] Z. Chen, Z. Xu, J. Du, and M. Mei, "Efficient Encoding for Bounded Model Checking of Timed Automata," *IEEJ Transactions on Electrical and Electronic Engineering*, vol. 12, no. 5, pp. 710–720, 2017.

[31] T. Yokogawa, M. Kondo, H. Miyazaki, S. Amasaki, Y. Sato, and K. Arimoto, "Bounded model checking of Time Petri Nets using SAT solver," *IEICE Electronics Express*, vol. 12, no. 2, p. 20141112, Jan. 2015.

[32] S. Ogata, T. Tsuchiya, and T. Kikuno, "SAT-Based Verification of Safe Petri Nets," in *Proc. of the Second Int'l Conf. on Automated Technology for Verification and Analysis (ATVA 2004)*, no. October 2004, 2004, pp. 79–92.

[33] N. Igawa, T. Yokogawa, S. Amasaki, K. Komoku, Y. Sato, and K. Arimoto, "Interpolation Based Unbounded Model Checking for Time Petri Nets," in *Proc. of 2018 IEEE 7th Global Conf. on Consumer Electronics (GCCE)*, 2018, pp. 587–591.

[34] S. Cotton, and O. Maler, "Fast and Flexible Difference Constraint Propagation for DPLL(T)," in *Proc. of the 9th Int'l Conf. Theory and Applications of Satisfiability Testing (SAT 2006)*, vol. 4121, 2006, pp. 170–183.

[35] A. Lazaro, D. Girbau, and R. Villarino, "Analysis of vital signs monitoring using an ir-uwb radar," *Progress In Electromagnetics Research*, vol. 100, pp. 265–284, 2010.

[36] J. W. Mason, D. J. Ramseth, D. O. Chanter, T. E. Moon, D. B. Goodman, and B. Mendzelevski, "Electrocardiographic reference ranges derived from 79,743 ambulatory subjects," *Journal of Electrocardiology*, vol. 40, no. 3, pp. 228 – 234.e8, 2007.

[37] 本間 研一，大森 治紀，大橋 俊夫，河合 康明，黒沢 美枝子，鯉淵 典之，伊佐 正，小澤 瀞司，福田 康一郎，標準生理学，8th ed.，ser. Standard textbook　医学書院，2014.

[38] SAKURA TECH CO., LTD., "miRadar," https://sakuratech.jp/.

[39] LIFE SENSOR CO., LTD., "UWB sensor," http://www.lifesensor.co.jp/.

[40] UNION TOOL CO., "myBeat," http://www.uniontool-mybeat.com/.

[41] 高田 晴子，高田 幹夫，金山 愛，"心拍変動周波数解析の LF 成分・HF 成分と心拍変

動係数の意義”，総合健診，vol. 32，no. 6，pp. 504–512，2005.

[42] O. Odemuyiwa, M. Malik, T. Farrell, Y. Bashir, J. Poloniecki, and J. Camm, “Comparison of the predictive characteristics of heart rate variability index and left ventricular ejection fraction for all-cause mortality, arrhythmic events and sudden death after acute myocardial infarction,” *The American Journal of Cardiology*, vol. 68, no. 5, pp. 434 – 439, 1991.

[43] 神一敬，加藤量広，鈴木菜摘，中里信和，“焦点発作の側方診断と自律神経”，臨床神経生理学，vol. 46，no. 6，pp. 585–590，2018.

[44] S. L. Moshé, E. Perucca, P. Ryvlin, and T. Tomson, “Epilepsy: new advances,” *The Lancet*, vol. 385, no. 9971, pp. 884–898, 2015.

[45] K. L. McMillan, “Interpolation and SAT-Based Model Checking,” in *Proc. of the 15th Int’l Conf. on Computer Aided Verification (CAV 2003)*, 2003, pp. 1–13.

[46] J. Sifakis, “Performance evaluation of systems using nets,” in *Net Theory and Applications, LNCS 84*, 1980, pp. 307–319.

[47] J. Dubrovin, T. Junttila, and K. Heljanko, “Exploiting step semantics for efficient bounded model checking of asynchronous systems,” *Science of Computer Programming*, vol. 77, no. 10-11, pp. 1095–1121, 2012.

[48] “SMT-COMP 2018,” http://smtcomp.sourceforge.net/2018/.

[49] R. Bruttomesso, A. Cimatti, A. Franzén, A. Griggio, and R. Sebastiani, “The MathSAT 4 SMT Solver,” in *Proc. of the 20th Int’l Conf. on Computer Aided Verification (CAV 2008)*, 2008, pp. 299–303.

[50] L. De Moura, and N. Bjørner, “Z3: An efficient SMT Solver,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4963 LNCS, pp. 337–340, 2008.

[51] J. Christ, J. Hoenicke, and A. Nutz, “SMTInterpol : an Interpolating SMT Solver,” in *Proc. of 19th Int’l SPIN Workshop on Model Checking of Softw. (SPIN 2012)*, 2012, pp. 248–254.

[52] B. Dutertre, “Yices 2.2,” in *Proc. of 26th Int’l Conf. on Computer Aided Verification (CAV 2014)*, 2014, pp. 737–744.

[53] C. Barrett, C. L. Conway, M. Deters, L. Hadarean, D. Jovanovi, T. King, A. Reynolds, and C. Tinelli, “CVC4,” in *Proc. of 23rd Int’l Conf. on Computer Aided Verification (CAV 2011)*, 2011, pp. 171–177.

[54] M. van Gastel, S. Stuijk, and G. de Haan, “Robust respiration detection from

remote photoplethysmography," *Biomedical Optics Express*, vol. 7, no. 12, pp. 4941–4957, 2016.