プロトコル仕様誤りの体系的分類とプロトコル検証

5T-4

角田 良明, 若原 恭, 乗越 雅光

国際電信電話株式会社

1. まえがき

プロトコル仕様の誤りを検出するプロトコル検証技術は、信頼性の高い通信ソフトウェアを開発する上で極めて重要な技術である。そのため、仕様誤りを検出する様々なプロトコル検証法が提案されている。しかし、従来の研究では、限られた代表的な仕様誤りを個別に検出する検証法の提案に留まっていた。その理由は一般的な仕様誤りの厳密な定義を与えていなかったからである。本稿では、一般的な仕様誤りの厳密な定義を与えた後、その定義に従って仕様誤りを体系的に分類した結果を示す。この分類の特徴は、任意の仕様誤りをsafetyとlivenessの概念で体系的に分類している点にある。また、この分類は仕様誤りを検出するための計算複雑さによる分類にもなっている。

2. プロトコル仕様

［定義1］ プロトコル仕様は、次の4項組で定義する。$P=(Q, o, M, succ)$, $Q=(Q_1, \cdots, Q_N)$, $o=(o_1, \cdots, o_N)$, $M=(M_{11}, \cdots, M_{NN})$, $succ=(succ_1, \cdots, succ_N)$, $succ_i : Q_i \times (M_{ij} \cup M_{ji}) \rightarrow Q_i$ $(1 \leqq i \leqq N)$。ここで、Nはプロセス数、Q_i はプロセスiの状態の集合、$o_i \in Q_i$ はプロセスiの初期状態、M_{ij} $(i \neq j)$ はプロセスiからプロセスjへ伝送されるメッセージの集合、$succ_i$ はメッセージ$m_i \in M_{ij} \cup M_{ji}$の送信あるいは受信によるプロセスiの次状態関数を表す。(s_i, x) の対を遷移という。$x \in M_{ij}$ ならばこの対を送信遷移という。$x \in M_{ji}$ならばこの対を受信遷移という。以降では、プロトコル仕様を単に仕様という。

［定義2］ プロトコル仕様のグローバル状態を$G=(S, C)$で表す。ここで、$S=(s_1, \cdots, s_N)$, $C=(c_{11}, \cdots, c_{NN})$, $s_i \in Q_i$ $(1 \leqq i \leqq N)$, $c_{ij} \in M_{ij}^*$ $(1 \leqq j \leqq N, 1 \leqq j \leqq N, i \neq j)$ とする。ϵは空系列を表す。$G_0=(S_0, C_0)$, $S_0=(o_1, \cdots, o_N)$, $C_0=(\epsilon, \cdots, \epsilon)$ のとき、G_0 は初期グローバル状態という。

［定義3］グローバル状態$G=(S, C)$から$G'=(S', C')$へのグローバル遷移を$G \Rightarrow G'$で表す。$G \Rightarrow G'$であるための必要十分条件は条件①：［$s_i' = succ_i(s_i, x)$, $c_{ij}' = c_{ij} \cdot x$を満たすi, j, xが存在する。それ以外の要素はかわらない。このとき、$G \Rightarrow G'$ by (s_i, x)とかく］、あるいは、条件②：［$s_j' = succ_j(s_j, x)$, $c_{ji}' = x \cdot c_{ji}$を満たすi, j, xが存在する。それ以外の要素はかわらない。このとき、$G \Rightarrow G'$ by (s_j, x)とかく］を満たすことである。これらの条件において、・は系列の連結を表す。更に、$G_1 \Rightarrow G_2 \Rightarrow \cdots \Rightarrow G_n$ であるn $(\geqq 1)$ が存在するときG_n はG_1 より到達可能であるという。$G_1 = G_0$ のときG_n は単に到達可能であるという。到達可能な全てのグローバル状態$G=(S, C)$において、全てのチャネルに蓄積されるメッセージの系列の長さ、即ち、全てのi, jに対するc_{ij}の長さが有限であれば、仕様は有限であるという。

［定義4］ $succ_i(s_i, x) \in Q_i$ を満たす$succ_i$ が定義されているとき、送信遷移あるいは受信遷移 (s_i, x) が仕様定義されているという。s_i を含む$G=(S, C)$が到達可能であるとき、送信遷移 (s_i, x) が実行可能であるという。s_i を含む$G=(S, C)$が到達可能であり、かつ$c_{ji}=x \cdot \cdots$を満たすjとxが存在するとき、受信遷移 (s_i, x) が実行可能であるという。

［定義5］ 遷移系列 $(t^1, x^1) \cdot (t^2, x^2) \cdot \cdots \cdot (t^n, x^n)$がグローバル状態Gからグローバル状態G'への長さnの実行可能遷移系列であるための必要十分条件は、条件①：［Gは到達可能である］、かつ、条件②：［$G^i \Rightarrow G^{i+1}$ by (t^i, x^i)。但し、$1 \leqq i \leqq n$, $G^1 = G$, $G^{n+1} = G'$］を満たすことである。

3. 仕様誤りの意味による分類

本節では、実行可能遷移系列に基づいた仕様誤りの厳密な定義を与えた後、任意の仕様誤りに対し仕様がその仕様誤りを含まないという性質は、以降で定義するsafetyとlivenessという性質で全て特徴づけられることを示す。

［定義6］ 任意に与えられた仕様Pにおいて、初期グローバル状態からの実行可能遷移系列をσで表す。仕様Pに対し、与えられた”σに関する述語”を満たすσの集合をAで表す。このようなσに関する述語を性質とよび、$p(A)$で表す。仕様Pに対する全てのσの集合をBで表す。$B=A$であれば、Pに対し$p(A)$が成立するという。仕様誤りは、Pに対し$p(A)$が成立しない、即ち、”σに関する述語”を満たさない、仕様の要素及びそれに基づいて定義されたもの、即ち、状態、遷移、グローバル状態、遷移系列などをいう。

［定義7］ 仕様の性質$p(A)$がsafetyであるための必要十分条件は初期グローバル状態からの任意の実行可能遷移系列$\sigma=(t^1, x^1) \cdot (t^2, x^2) \cdot \cdots \cdot (t^n, x^n)$に対し、$\sigma \notin A$であれば、任意の実行可能遷移系列$\beta$に対し、$(t^1, x^1) \cdot (t^2, x^2) \cdot \cdots \cdot (t^j, x^j) \cdot \beta \notin A$であるような$\sigma$の部分系列 $(t^1, x^1) \cdot (t^2, x^2) \cdot \cdots \cdot (t^j, x^j)$ $(1 \leqq j \leqq n)$ が存在することである。

［定義8］ 仕様の性質$p(A)$がlivenessであるための必要十分条件は初期グローバル状態からの任意の実行可能遷移系列$\alpha=(t^1, x^1) \cdot (t^2, x^2) \cdot \cdots \cdot (t^n, x^n)$に対し、$\alpha \notin A$であ

Systematic Classification of Protocol Specification Errors and Protocol Validation

Yoshiaki Kakuda, Yasushi Wakahara and Masamitsu Norigoe

Kokusai Denshin Denwa Co., Ltd.

れば、$(t^1,x^1)\cdot(t^2,x^2)\cdot\cdots\cdot(t^j,x^j)\cdot\beta\in A$を満たす$\alpha$の部分系列$(t^1,x^1)\cdot(t^2,x^2)\cdot\cdots\cdot(t^j,x^j)$ $(1\leqq j\leqq n)$と実行可能遷移系列βが存在することである。

文献[1,3]のlivenessの定義と異なることに注意されたい。定義7、8の意味について述べる。safetyの場合、実行可能遷移系列σに関して仕様誤りが検出されたら、σを逆戻ったグローバル状態にどのような実行可能遷移系列βを連結しても、やはり仕様誤りが検出されるという回復不可能なσの部分系列が存在することを意味している。livenessの場合、実行可能遷移系列αに関して仕様誤りが検出されたら、αを逆戻ったグローバル状態に適当な実行可能遷移系列βを連結すれば、仕様誤りが検出されないという回復可能なαの部分系列が存在することを意味している。

［定理1］ 仕様の任意の性質はsafety、liveness、あるいは、これらの性質の両者で表すことができる。

この定理は定義7と定義8のsafetyとlivenessの定義が相補的であることより証明可能である。

以降では、仕様誤りの代表例として、未定義受信、実行不能送受信がないという性質はsafetyあるいはlivenessであることを示す。

［定義9］ 未定義受信がないという性質p_1は、全ての実行可能な受信遷移が仕様定義されていることである。

［命題1］ 定義9に示した性質p_1はsafetyである。

（略証） 初期グローバル状態からの長さnの任意の実行可能遷移系列を$\sigma=(t^1,x^1)\cdot(t^2,x^2)\cdot\cdots\cdot(t^n,x^n)$とする。$\sigma$により到達可能なグローバル状態を$G=(S,C)$，$S=(s_1,\cdots,s_N)$とする。$p_1$は、”S上の状態$s_i$ $(1\leqq i\leqq N)$を含む受信遷移が実行可能であれば仕様定義されている”と表すことができる。すると、この性質がsafetyであることはnに関する帰納法で証明できる。σにより(s_i,x)が実行可能だが仕様定義されていないと判定されれば、σ以外の実行可能遷移系列により上述のs_iを含むグローバル状態に到達しても(s_i,x)は仕様定義されていないので未定義受信である。

［定義10］ 実行不能送受信がないという性質p_2は、全ての仕様定義されている送信遷移あるいは受信遷移が実行可能であることである。

［命題2］ 定義10に示した性質p_2はlivenessである。

（略証） 初期グローバル状態からの長さnの任意の実行可能遷移系列を$\alpha=(t^1,x^1)\cdot(t^2,x^2)\cdot\cdots\cdot(t^n,x^n)$とする。$\alpha$により到達可能なグローバル状態を$G=(S,C)$，$S=(s_1,\cdots,s_N)$，とする。$p_2$は、”S上の状態$s_i$ $(1\leqq i\leqq N)$を含む送信遷移あるいは受信遷移が仕様定義されていれば実行可能である”と表すことができる。すると、この性質がlivenessであることはnに関する帰納法で証明できる。αにより(s_i,x)が仕様定義されているが実行可能でないと判定されても、α以外の実行可能遷移系列により上述のs_iを含むグローバル状態に到達すれば、(s_i,x)は実行可能となり得るので実行不能送受信とは限らない。

4．仕様誤りの計算複雑さによる分類

本節では、仕様誤りを検出するための計算複雑さについて論ずる。これまでに、次の事実が証明されている。

［事実1］[2] 一般に、任意の仕様に対し仕様誤りを検出するプロトコル検証法は存在しない。これに対して、有限である仕様に対し仕様誤りを検出するプロトコル検証法は存在する。

従って、以降では、有限である仕様に対するプロトコル検証法について計算複雑さを論ずる。

定義6より、一般に、プロトコル検証法は、実行可能遷移系列を列挙する部分とこれらの系列に関する性質を検査する部分で構成されると考えられる。

定理1より、仕様誤りがないという性質はsafetyとlivenessで分類できることを示した。実は、この分類は仕様誤りを検出するための計算複雑さによる分類にもなっている。実行可能遷移系列を列挙する部分の検出法を比較すると、safetyが成立しない仕様誤りを検出する場合には、必ずしも全ての実行可能遷移系列を列挙する必要はないが、livenessが成立しない仕様誤りを検出する場合には、常に全ての実行可能遷移系列を列挙する必要があるからである。これについて詳しく述べる。

safetyが成立しない仕様誤りは、その性質を満たさない実行可能遷移系列を少なくとも一つ検出すれば、直ちにその誤りを検出できる。これに対して、livenessが成立しない仕様誤りは、全ての実行可能遷移系列に対しその性質を満たさないならば、最後にその誤りを検出することができる。例えば、実行可能で仕様定義されていない遷移をもつグローバル状態に到達した実行可能遷移系列が存在すれば直ちに未定義受信が検出される。これに対して、仕様定義されているが実行可能でない遷移をもつグローバル状態に到達した実行可能遷移系列が存在しても、全ての実行可能遷移系列を列挙し終えなければ、実行不能送受信と断定することはできない。

以上の結果をまとめると、次の定理が成立する。

［定理2］ livenessが成立しない仕様誤りを検出する計算複雑さはsafetyが成立しない仕様誤りを検出する計算複雑さより複雑である。

5．あとがき

本稿では、実行可能遷移系列に関する任意の仕様誤りをsafetyとlivenessの概念に基づいて体系的に分類した。また、この分類はこのような性質が成立しないという仕様誤りを検出するための計算複雑さによる分類になっていることも示した。この結果により、任意に与えられた仕様誤りがどの分類に入るのかを判定することにより、それを検出するためのプロトコル検証の計算複雑さを把握することが可能となった。更に、本稿の結果に基づいて、任意の仕様誤りを検出するプロトコル検証を実現することも可能であるが、これについては別途報告する。最後に、日頃御指導、御鞭撻頂くＫＤＤ研究所、野坂所長、小野次長に感謝する。また、熱心に御討論頂いた交換システム研究室、森前室長、池田主任研究員をはじめとする研究室諸兄に感謝する。

文献

[1] B.Alpern and F.B.Schneider:"Defining liveness", Information Processing Letters, 21, pp.181-185 (Oct.1985).
[2] D.Brand and P.Zafiropulo:"On communicating finite-state machines", IBM Res. Rep. RZ1053 (1981).
[3] S.S.Lam and A.U.Shankar:"Protocol verification via projections", IEEE Trans. on Soft. Eng., SE-10, 4, pp.325-342 (July 1984).