社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (35)
2006／7／21

限定並行ブラックボックス零知識証明のラウンド数下界

村谷 博文

(株) 東芝 研究開発センター 川崎市幸区小向東芝町1
E-mail: hirofumi.muratani@toshiba.co.jp

あらまし プレインモデルにおける、自己合成の場合の m-限定並行零知識証明プロトコルのラウンド数の下界を導出する。これは、非限定並行の場合の Canetti-Kilian-Petrank-Rosen の結果を m-限定並行に拡張したものである。結果として得られたラウンド数下界は $o(\frac{\log m}{\log\log m})$ である。我々が先の研究で得た一般合成の場合のラウンド数の上界（プロトコルが存在する十分条件）$\omega(\log m)$ と合わせて考えると、漸近的オーダとしてほぼ $\log m$ が最適であることが分かる。

キーワード 並行ブラックボックス零知識，限定並行性，ラウンド計算量

Asymptotic Lower Bound on Round Complexity of Bounded Concurrent Black-Box Zero-Knowledge Proof Protocols

Hirofumi MURATANI

Corporate Research & Development Center, Toshiba Corporation
1, Komukai-Toshiba-cho, Saiwai-ku, Kawasaki 212-8582, Japan
E-mail: hirofumi.muratani@toshiba.co.jp

Abstract We derive a lower bound on the round complexity of an m-bounded concurrent black-box zero-knowledge interactive proof protocol. This is an extension of the result of the Canetti-Kilian-Petrank-Rosen to the case of m-bounded concurrency. The resulting bound is $o(\frac{\log m}{\log\log m})$. Considering it together with our previous result on an upper bound $\omega(\log m)$, we can conclude that the asymptotic order almost $\log m$ is optimal.

Key words concurrent black-box zero-knowledge, bounded concurrency, round complexity

1. はじめに

零知識対話証明（ZKIP）は基本的な暗号プロトコルのひとつのため，その合成が詳しく研究されてきた[1]～[12]．特に，Canetti-Kilian-Petrank-Rosen [9] は，plain model において非自明言語に対する並行ブラックボックス ZKIP（cBBZKIP）のラウンド数下界を示し，定数ラウンドの不可能性を証明した．本稿では，各セッションに対して，その実行中に並行して実行されるセッションを m 個以内に制限した，m-限定並行（m-bounded concurrency）ブラックボックス ZKIP（m-cBBZKIP）のラウンド数下界を示す．

2. 準 備

$Poly$ を正多項式関数全体とする．$[n]=\{1,\cdots,n\}$ とする．$Negl(k)$ は k に関して無視できる関数全体とする．確率変数族 $X=\{X(x)\}_{x\in\{0,1\}^*}$ と $Y=\{Y(x)\}_{x\in\{0,1\}^*}$ が，任意の確率性多項式時間アルゴリズム D に対して $|\Pr[D(X(x),x)=1] - \Pr[D(Y(x),x)=1]| \in Negl(|x|)$ のとき，X と Y は計算量的識別不可能であるといい，$X \stackrel{c}{\equiv} Y$ で表す．

[定義 1]（cBBZKIP [9]） (P,V) を言語 $L\subset\{0,1\}^*$ に対する対話証明系，$x\in\{0,1\}^*$ を P と V の共通入力，セキュリティ・パラメータ k を x のサイズ $|x|$ とする．任意の $n(\cdot)\in Poly$ に対して，k と $n(k)$ に関する多項式時間アルゴリズム（シミュレータ）S が存在し，高々 $n(k)$ セッションをそれぞれの P と並行実行する任意の多項式時間アルゴリズム（攻撃者）V^* に対して，$\mathrm{view}^P_{V^*} \stackrel{c}{\equiv} S^{V^*}$ を満たすとき，(P,V) は cBBZKIP であるという．ここで，$\mathrm{view}^P_{V^*} = \{\mathrm{view}^P_{V^*}(x)\}_{x\in L}$ は対話履歴と V^* の乱数テープの内容からなる確率変数族，$S^{V^*} = \{S^{V^*}(x)\}_{x\in L}$ は V^* へのブラックボックスアクセスが許された S の出力を表す確率変数族とする．

[定義 2]（m-限定並行性） 各セッションの実行中に自己を含め高々 m セッションがメッセージ送信する合成を m-限定並行といい，m-限定並行の cBBZKIP を m-cBBZKIP と呼ぶ．

アルゴリズム 1 再帰ブロックのスケジュール

```
1: procedure R(μ)
2:     if μ ≦ k then
3:         for s ← 1, μ do
4:             セッション s を完了まで実行する
5:         end for
6:     else
7:         for j ← 1, r + 1 do
8:             最初の k 個のセッションの各々で v_j と p_j を交換する
9:             if j < r + 1 then
10:                R(⌊(μ−k)/r⌋)
11:            end if
12:        end for
13:    end if
14: end procedure
```

3. 非限定並行の下界

まず，Canetti らが示したラウンド数下界 [9] をレビューする．

[定理 1]（Canetti et al. [9]） $r : \mathbb{N} \to \mathbb{N}$ を $r(n) = o\left(\frac{\log n}{\log \log n}\right)$ なる関数，n をセッション数とする．言語 L に対する $r(n)$-ラウンド cBBZKIP が存在するならば，$L \in \mathcal{BPP}$ である．

[定義 3]（ラウンド） r-ラウンドプロトコルは，$2r+2$ 個のメッセージを交換する：

（1） v_1：固定の検証者メッセージ．

（2） p_1：証明者の回答メッセージ．

（3） $\mathrm{v}_2, \mathrm{p}_2, \cdots, \mathrm{v}_r, \mathrm{p}_r$：交互に検証者／証明者メッセージ．

（4） $\mathrm{v}_{r+1} \in \{\mathtt{ACCEPT}, \mathtt{REJECT}\}$：検証者メッセージ．

（5） p_{r+1}：証明者の固定の通知メッセージ．

[定義 4]（クエリ／回答） S から V^* へのメッセージをクエリと，V^* から S へのメッセージを回答と呼ぶ．クエリは，P と V の対話履歴の形式で，証明者メッセージで終わる．回答は，1 個の検証者メッセージである．以下を仮定する：

（1） S は，同じクエリを二度繰り返さない．

（2） S は，$\bar{q}$ のクエリ以前に，$\bar{q}$ の接頭語をクエリしている．

（3） S は，$\bar{q}$ の出力以前に，$\bar{q}$ をクエリしている．

[定義 5]（スケジュール） セッション数を $n = k^2$ とする（定理の証明には，この場合だけで十分である）．$\mathcal{R}(k^2)$ のスケジュールに従って対話が行われるとする．$\mathcal{R}(\cdot)$ を再帰ブロックと呼び，アルゴリズム 1 で定義する．$\mathcal{R}(\cdot)$ の 8 行目で処理される k 個のセッションをメインセッションと呼ぶ．各セッションに指標 $(\ell, i) \in [k] \times [k]$ を割り当てる．(ℓ, i) は，そのセッションが第 ℓ 再帰ブロックの第 i メインセッションであることを表す．

[定義 6]（次メッセージ識別子への写像） スケジュール $\mathcal{R}(k^2)$ により，対話履歴 $\bar{q} = (b_1, a_1, \cdots, b_t, a_t)$ から次の検証者メッセージの識別子への写像 π_{sn} と π_{msg} が定義できる：

（1） $\pi_{sn}(\bar{q}) = (\ell, i) \in [k] \times [k]$：次の検証者メッセージは，セッション (ℓ, i) に属する．

（2） $\pi_{msg}(\bar{q}) = j \in [r+1]$：次の検証者メッセージは，そのセッション中の j 番目の検証者メッセージ $\mathrm{v}_j^{(\ell,i)}$ である．

[定義 7]（ブロック接頭語） $\pi_{sn}(\bar{q}) = (\ell, i)$ なるクエリ $\bar{q}$ に対して，$\bar{q}$ の接頭語 $bp(\bar{q})$ が，$\pi_{sn}(bp(\bar{q})) = (\ell, 1)$ かつ $\pi_{msg}(bp(\bar{q})) = 1$ を満たすとき，$bp(\bar{q})$ を $\bar{q}$ のブロック接頭語と呼ぶ．$bp(\bar{q})$ は再帰ブロック番号 ℓ に対応すると言う．

アルゴリズム 2 V^* の戦略

```
1: procedure V*(x, q̄ = (b_1, a_1, ···, b_t, a_t))
2:     if q is not legal then
3:         ERROR メッセージを発して停止する
4:     else if a_t がある再帰ブロックの p_{r+1}^{(k)} の形である then
5:         if そのブロックの受理メインセッションが k^{1/2}/4 個未満で
               ある then
6:             DEVIATION メッセージを発して停止する
7:         end if
8:     end if
9:     bp(q̄) = (b_1, a_1, ···, b_γ, a_γ), (ℓ, i) = π_sn(q̄), j = π_msg(q̄),
           ip(q̄) = (b_1, a_1, ···, b_δ, p_{j−1}^{(k)}), q̄ 内のセッション i の j − 1
           個の証明者メッセージ p_1^{(i)}, ···, p_{j−1}^{(i)} を決定する
10:    if j = 1 then
11:        セッション i に対する固定の最初の検証者メッセージ v_1^{(i)}
               を回答する
12:    else if j > 1 then
13:        b_{i,j} = g(i, ip(q̄)) を決定する
14:        if b_{i,j} = 0 then
15:            v_j^{(i)} = ABORT と設定する
16:        else if b_{i,j} = 1 then
17:            r_i = h(i, bp(q̄)) を決定する
18:            v_j^{(i)} = V(x, r_i; p_1^{(i)}, ···, p_{j−1}^{(i)}) を計算する
19:        end if
20:        v_j^{(i)} を回答する
21:    end if
22: end procedure
```

[定義 8]（反復接頭語） $\pi_{sn}(\bar{q}) = (\ell, i)$ かつ $\pi_{msg}(\bar{q}) = j (> 1)$ なるクエリ $\bar{q} = (b_1, a_1, \cdots, b_t, a_t)$ に対して，$\bar{q}$ の接頭語 $ip(\bar{q}) = (b_1, a_1, \cdots, b_\delta, a_\delta)$ が，セッション (ℓ, k) の第 $(j-1)$ 証明者メッセージ $a_\delta = \mathrm{p}_{j-1}^{(\ell,k)}$ で終わるとき，$ip(\bar{q})$ を $\bar{q}$ の反復接頭語と呼ぶ．$ip(\bar{q})$ は $\bar{q}$ のブロック接頭語に対応すると言う．

[定義 9]（V^* の戦略） S が多項式 $t_S(k)$ 時間限定であるとする．G を $\{0,1\}^{\mathrm{poly}(k)}$ から $\{0,1\}$ への $t_S(k)$-wise 独立ハッシュ関数族とし，$\forall \alpha \in \{0,1\}^{\mathrm{poly}(k)}$ $\Pr_{g \leftarrow G}[g(\alpha)=1] = k^{-\frac{1}{2r}}$ とする．H を $\{0,1\}^{\mathrm{poly}(k)}$ から $\{0,1\}^{\rho_V(k)}$ への $t_S(k)$-wise 独立ハッシュ関数族とする．V^* の戦略をアルゴリズム 2 に示す．

セッション $(\ell, i) = \pi_{sn}(\bar{q})$ において P への回答を計算するために用いる乱数性は，再帰ブロック番号 ℓ に対応するブロック接頭語 $bp(\bar{q})$ にハッシュ関数 $h \in H$ を適用して生成される．

V がセッション $(\ell, i) = \pi_{sn}(\bar{q})$ を中止するか否かを決定するための乱数性は，スケジュールが次の検証者メッセージ j に到達する毎にクエリ $\bar{q}$ の反復接頭語 $ip(\bar{q})$ にハッシュ関数 $g \in G$ を適用して生成される．

[定義 10]（L の判定アルゴリズム） L の確率性多項式時間判定アルゴリズム D をアルゴリズム 3 とする．

3.1 完全性

[補題 1] 有限個を除きすべての $x \in L$ に対して，アルゴリズ

アルゴリズム 3 L の判定アルゴリズム

```
procedure D(x ∈ {0,1}^k)
    g ←R G と h ←R H を選ぶ
    S(x) を呼び出し V* へのブラックボックスアクセスを与える
    S(x) が正当な対話履歴を出力するとき受理し，そうでないとき拒否する
end procedure
```

ム D は少なくとも 2/3 の確率で x を受理する．確率は，g と h と S のコインの上でとられる．

[定義 11] (deviation gap) D を (P, V^*) の対話履歴とシミュレータ S^{V^*} が生成した対話履歴を識別するアルゴリズムとし，D の deviation gap Δ_D と S の deviation gap Δ を定義する：

$$\Delta_D = \Pr[D(S^{V^*}(x), x) = 1] - \Pr[D(\mathrm{view}^P_{V^*}(x), x) = 1],$$
$$\Delta = \max_{D \text{ is PPT}} \{\Delta_D\}$$

[補題 1 の証明] $x \in L$, $g \xleftarrow{R} H$, $h \xleftarrow{R} H$ とし，以下を示す：

(1) g の一様性により g が 1 を出力する確率が $k^{-1/2r}$ であることから，V^* が P との対話中に，DEVIATION メッセージの出力がないと仮定して，そのセッションを中断せずに完了する確率は，$(k^{-1/2r})^r = k^{-1/2}$ である．

V^* と P の間のこの対話は，DEVIATION メッセージの出力がなく V^* が現在のセッションを停止しないと仮定すると，h の一様性により V と P の間の対話と同じ分布をする．V と P の間の cBBZKIP の完全性により，V がこのセッションの対話を受理する確率は少なくとも 1/2 である．ゆえに，DEVIATION メッセージの出力がないと仮定して，V^* がこのセッションを中断することなく受理する確率は，少なくとも $\frac{1}{2} \times k^{-1/2} = \frac{k^{-1/2}}{2}$ となる．

ある再帰ブロックの各メインセッションが受理される確率は，それ以前に DEVIATION を出力したメインセッションがなかったと仮定して，少なくとも $\frac{k^{-1/2}}{2}$ であるから，受理メインセッションの個数の期待値は，少なくとも $\sum_{i=1}^{k} \frac{k^{-1/2}}{2} = \frac{k^{1/2}}{2}$ である．Chernoff の下界を用いると，そのブロックが少なくとも $\frac{k^{-1/2}}{2}$ 個のメインセッションを受理する確率は少なくとも $1 - e^{\Omega(n^{1/2})}$ となる．よって，すべての再帰ブロックが少なくとも $\frac{k^{-1/2}}{2}$ 個のメインセッションを受理する確率は少なくとも $(1 - e^{\Omega(n^{1/2})})^n > 1 - n \cdot e^{-\Omega(n^{1/2})}$ となる．ゆえに，V^* が P との対話において DEVIATION メッセージを出力する確率は無視できる．

零知識性により，ある S が存在して，すべての g, h に対して，$S^{V^*} \stackrel{c}{\equiv} \mathrm{view}^P_{V^*}$ となる．ゆえに，$g \xleftarrow{R} G$, $h \xleftarrow{R} H$ のときも，$S^{V^*} \stackrel{c}{\equiv} \mathrm{view}^P_{V^*}$ となる．よって，有限個を除きすべての $x \in L$ に対して，Δ を高々1/4 とできる．

以上より，有限個を除きすべての $x \in L$ に対して，D が $x \in L$ を受理しない確率は，高々1/4 に無視できる関数を加えたものである．つまり，有限個を除きすべての $x \in L$ に対して，D は少なくとも 2/3 の確率で x を受理する．

□

アルゴリズム 4 P^* の処理

```
procedure P*(x)
    (σ, g, h) を一様に選ぶ．
    (ξ, η) ∈ {1,···,q_S(k)} × {1,···,k} を一様に選ぶ．k = |x| で，q_S(k) < t_S(k) は S によるクエリの回数の上限とする．
    S_σ^{V,g,h(r)}(x) のエミュレートを開始する．
    while S がクエリ q̄ = (b_1, a_1, ···, b_t, a_t) を行う do
        bp(q̄) = (b_1, a_1, ···, b_γ, a_γ), (ℓ, i) = π_sn(q̄), j = π_msg(q̄), ip(q̄) = (b_1, a_1, ···, b_δ, p^(i)_{j-1}), q̄ 中の p^(i)_1, ···, p^(i)_{j-1} を決定する．
        if j = 1 then 最初の固定の検証者メッセージを S に回答する．
        else if j > 1 then b_{i,j} = g(i, ip(q̄)) を決定する．
        end if
        if bp(q̄) は ξ 番目ブロック接頭語である ∧ i = η then
            if b_{i,j} = 0 then S に ABORT を回答する．
            else if b_{i,j} = 1 then
                if (j − 1) 番目メッセージを V(x, R) に送信済み then
                    V の (j − 1) 番目回答を検索し S に回答する．
                else if (j − 1) 番目メッセージを V(x, R) に未送信 then
                    p^(i)_{j-1} を V(x, R) に転送し，V(x, R) の回答を S に回答する．
                end if
            end if
        else if bp(q̄) は ξ 番目ブロック接頭語でない ∨ i ≠ η then
            if b_{i,j} = 0 then S に ABORT を回答する．
            else if b_{i,j} = 1 then
                r_i = h(i, bp(q̄)) を決定する．
                S に V(x, r_i; p^(i)_1, ···, p^(i)_{j-1}) を回答する．
            end if
        end if
    end while
end procedure
```

3.2 健全性

[補題 2] 有限個を除きすべての $x \notin L$ に対して，処理 D は少なくとも 2/3 の確率で x を拒否する．確率は，g と h と S のコイン σ の上でとられる．

[補題 2 の証明] V に $x \notin L$ を受理させる証明者 P^* をアルゴリズム 4 で定義する．P^* は，S をエミュレートし，あるセッションを $V(x, R)$ に受理させようとする．ここで，R は V のランダムコインとする．V^* は，それ以外のセッションに対しては，h が生成するランダムコインを用いる．

3.4 節の補題 3 は，S の成功確率が無視できないと仮定すると，P^* の成功確率も無視できないことを示している．$x \notin L$ のとき，これは (P, V) の健全性の仮定に反する．従って，$x \notin L$ のとき，S が $V(x, R)$ に受理させる確率は無視できる．

S は V^* を巻戻せるが，P^* は $V(x, R)$ を巻戻せないので，アルゴリズム 4 において，P^* が以前 $V(x, R)$ に転送したメッセージとは異なるメッセージでステップ 13 に達した場合，新

しいメッセージに対する $V(x,R)$ の回答は以前の回答とは異なるため，P^* はステップ 13 で失敗する．しかし，3.3 節の補題 2 と 3.5 節の補題 4 は，P^* がステップ 13 でそのような失敗をする確率が無視できることを示している．つまり，巻戻しにより $V(x,R)$ に同じメッセージを繰り返し転送する場合，無視できる確率を除き，以前の同じ内容のメッセージが転送されるか，ABORT されるかいずれかである． □

3.3 主張 2 とその証明

[定義 12]（シミュレータの実行） 入力 x，ランダムコイン σ が与えられ，$g \in G, h \in H$ の V^* へのオラクルアクセスを許されるとき，ミュレータ $S^{V^*}(x)$ が行ったクエリの系列を S の実行と定義し，$\mathrm{EXEC}_x(\sigma,g,h)$ と表す．

[定義 13] $\overline{bp}_\xi$ を $\mathrm{EXEC}_x(\sigma,g,h)$ 中に現れる ξ 番目のブロック接頭語とする．関数 $h^{(R)} = h^{(R,\sigma,g,h,\xi,\eta)}$ は，以下を満たす h' の集合 H' 中に分布しているとする：

$$h'(\eta',\overline{bp}_{\xi'}) = \begin{cases} R, & (\eta',\xi') = (\eta,\xi), \\ h(\eta',\overline{bp}_{\xi'}), & (\eta',\xi') \neq (\eta,\xi). \end{cases}$$

[主張 1] いかなる σ,g,ξ,η に対しても，h が H 内に一様に分布し，R が $\{0,1\}^{\rho_V(k)}$ 内に一様分布しているならば，$h^{(R)}$ も H 内に一様分布する．

[証明] H が $t_S(k)$-wise 独立ハッシュ関数族であることより，$q_S(k)$ 個の引数の各々に h を適用して得られる値の系列の分布は，同じ引数の系列に対して，真なランダム関数の族から一様に選択した関数を適用した値の系列と同じ分布をする．一方，R は，h の選択とは独立に，一様に選択される．仮に引数を適応的に選択することにより，$h^{(R)}$ を適用した系列の分布に影響を与えようとしても，H の $t_S(k)$-wise 独立性により不可能である．よって，$h^{(R)}$ も H 内に一様分布する． □

[定義 14]（ip-相違クエリ） $ip(\bar{q}_1) \neq ip(\bar{q}_2)$ を満たすクエリ $\bar{q}_1$ と $\bar{q}_2$ を ip-相違クエリであると言う．

[定義 15]（有用ブロック接頭語） $\mathrm{EXEC}_x(\sigma,g,h)$ 中に現れるブロック接頭語 $\overline{bp}$ が以下を満たすとき，i-有用と呼ぶ：

（1） すべての $j \in [r+1]\backslash\{1\}$ に対して，ブロック接頭語 $\overline{bp}$ に対応し，$\pi_{sn}(\bar{q}) = (\ell^{(\overline{bp})}, i)$，$\pi_{msg}(\bar{q}) = j$，$g(i, ip(\bar{q})) = 1$ を満たす ip-相違クエリ $\bar{q}$ の個数は厳密に 1 個である．

（2） ブロック接頭語 $\overline{bp}$ に対応し，$\pi_{sn}(\bar{q}) = (\ell^{(\overline{bp})}, i)$，$\pi_{msg}(\bar{q}) = r+1$，$g(i, ip(\bar{q})) = 1$ を満たす唯一のクエリ $\bar{q}$ は，V^* により ACCEPT で回答される．

i-有用となる $i \in [k]$ が存在するブロック接頭語を有用と呼ぶ．

[主張 2] $\mathrm{EXEC}_x(\sigma,g,h^{(R)})$ の ξ 番目ブロック接頭語が η-有用となる (σ,g,h,ξ,η) を P^* が選ぶとき，P^* は $V(x,R)$ を受理させる．

[証明] P^* が $V(x,R)$ へ転送する証明者メッセージは，セッション $(\ell^{(\overline{bp}_\xi)}, \eta)$ に対応し，$\mathrm{p}_{j-1}^{(\eta)}$ の形をしており，$\pi_{sn}(\bar{q}) = (\ell^{(\overline{bp}_\xi)}, \eta)$，$\pi_{msg}(\bar{q}) = j$，$g(\eta, ip(\bar{q})) = 1$ を満たすクエリ $\bar{q}$ に対応する．ξ 番目ブロック接頭語が η-有用という仮定より，上の条件 (1) より，すべての $j \in [r+1]\backslash\{1\}$ に対して，P^* が，相異なる $\mathrm{p}_{j-1}^{(\eta)}$ メッセージでステップ 13 に達することはない．特に，上の条件 (2) のクエリは，$V(x,R)$ に受理される． □

3.4 補題 3 とその証明

$x \in \{0,1\}^k\backslash L$ に対して，$S^{V^*}(x)$ が正当な対話履歴を出力する $(\sigma,g,h) \in \{0,1\}^* \times G \times H$ の集合を AC_x^k とする．

[補題 3] ある $p(\cdot) \in Poly$ に対し $\Pr_{\sigma,g,h}[(\sigma,g,h) \in \mathrm{AC}_x^k] > \frac{1}{p(k)}$ のとき $\Pr_{\sigma,g,h,\xi,\eta,R}[\langle P^*, V\rangle(x) = \mathrm{ACCEPT}] > \frac{1}{2p(k)q_S(k)k}$ である．

[補題 3 の証明] $\mathrm{EXEC}_x(\sigma,g,h)$ の ξ 番目ブロック接頭語が η-有用であることを $\mathrm{useful}_{\xi,\eta}(\sigma,g,h)$ と表記する．主張 2 より，

$$\Pr_{\substack{\sigma,g,h \\ \xi,\eta,R}}[\langle P^*, V\rangle(x) = \mathrm{ACCEPT}] \geq \Pr_{\substack{\sigma,g,h \\ \xi,\eta,R}}[\mathrm{useful}_{\xi,\eta}(\sigma,g,h^{(R)})].$$

主張 1 より，h と R が一様に選ばれるとき，(ξ,η) の値によらず $h^{(R)}$ は一様分布するので，$h^{(R)}$ は (ξ,η) とは独立である．よって，

$$\Pr_{\substack{\sigma,g,h \\ \xi,\eta,R}}[\mathrm{useful}_{\xi,\eta}(\sigma,g,h^{(R)})] = \Pr_{\substack{\sigma,g,h' \\ \xi,\eta}}[\mathrm{useful}_{\xi,\eta}(\sigma,g,h')].$$

一方，

$$\begin{aligned} &\Pr_{\substack{\sigma,g,h \\ \xi,\eta}}[\mathrm{useful}_{\xi,\eta}(\sigma,g,h)] \\ &\quad = \sum_{d=1}^{q_S(k)} \sum_{i=1}^{k} \Pr_{\substack{\sigma,g,h \\ \xi,\eta}}[\mathrm{useful}_{d,i}(\sigma,g,h) \wedge (\xi = d \wedge \eta = i)] \\ &\quad = \sum_{d=1}^{q_S(k)} \sum_{i=1}^{k} \Pr_{\sigma,g,h}[\mathrm{useful}_{d,i}(\sigma,g,h)] \cdot \Pr_{\xi,\eta}[\xi = d \wedge \eta = i] \\ &\quad \geq \Pr_{\sigma,g,h}[\exists i\ \mathrm{useful}_{d,i}(\sigma,g,h)] \cdot \frac{1}{q_S(k)\cdot k}. \end{aligned}$$

上の 3 つの式より，

$$\Pr_{\substack{\sigma,g,h \\ \xi,\eta,R}}[\langle P^*, V\rangle(x) = \mathrm{ACCEPT}] \geq \frac{\Pr_{\sigma,g,h}[\exists d \exists i\ \mathrm{useful}_{d,i}(\sigma,g,h)]}{q_S(k)\cdot k}.$$

ある多項式 $p(\cdot)$ に対して $\Pr[(\sigma,g,h) \in \mathrm{AC}_x^k] > \frac{1}{p(k)}$ なので，上式右辺の分子は，

$$\begin{aligned} &\Pr_{\sigma,g,h}[\exists d \exists i\ \mathrm{useful}_{d,i}(\sigma,g,h)] \\ &= 1 - \Pr_{\sigma,g,h}[\forall d \forall i\ \neg\mathrm{useful}_{d,i}(\sigma,g,h) \wedge (\sigma,g,h) \notin \mathrm{AC}_x^k] \\ &\quad - \Pr_{\sigma,g,h}[\forall d \forall i\ \neg\mathrm{useful}_{d,i}(\sigma,g,h) \wedge (\sigma,g,h) \in \mathrm{AC}_x^k] \\ &\geq 1 - \Pr_{\sigma,g,h}[(\sigma,g,h) \notin \mathrm{AC}_x^k] \\ &\quad - \Pr_{\sigma,g,h}[\forall d \forall i\ \neg\mathrm{useful}_{d,i}(\sigma,g,h) \wedge (\sigma,g,h) \in \mathrm{AC}_x^k] \\ &> \frac{1}{p(k)} - \Pr_{\sigma,g,h}[\forall d \forall i\ \neg\mathrm{useful}_{d,i}(\sigma,g,h) \wedge (\sigma,g,h) \in \mathrm{AC}_x^k]. \end{aligned}$$

後で示す補題 4 により，上式の右辺第 2 項は無視できるので，

$$\Pr_{\substack{\sigma,g,h \\ \xi,\eta,R}}[\langle P^*, V\rangle(x) = \mathrm{ACCEPT}] > \frac{1}{2\cdot p(k)\cdot q_S(k)\cdot k}.$$

□

3.5 補題 4 とその証明

[補題 4]

$$\Pr_{\sigma,g,h}[\forall d \forall i\ \neg\mathrm{useful}_{d,i}(\sigma,g,h) \wedge (\sigma,g,h) \in \mathrm{AC}_x^k] \in Negl(k).$$

[定義 16]（潜在的有用ブロック接頭語） $\mathrm{EXEC}_x(\sigma,g,h)$ 中の

次を満たすブロック接頭語 $\overline{bp}$ を潜在的有用と呼ぶ：

（1） ブロック接頭語 $\overline{bp}$ に対応する ip-相違クエリの個数は高々r^{c+1} である．

（2） S の実行は，ブロック接頭語 $\overline{bp}$ に対応するブロックの終わりまで到達する．

[補題 5] すべての $(\sigma,g,h)\in \mathrm{AC}^k_x$ に対して，$\mathrm{EXEC}_x(\sigma,g,h)$ は潜在的有用ブロック接頭語を含んでいる．

[定義 17]（クエリ-回答木） 頂点と辺が，それぞれ，検証者メッセージと証明者メッセージでラベル付けされたルート付きの木をクエリ-回答木と言う．ルートは最初のセッションの最初の固定の検証者メッセージに，ルートからの外向きの辺はそのセッションの最初の証明者メッセージに，木を下るパスはクエリに対応する．頂点から数えて ω 番目のレベルの頂点はスケジュール中の ω 番目の検証者メッセージを表している．同じレベルの姉妹の頂点の間の違いは，シミュレータの巻戻しにより生じた入力メッセージの違いである．

[定義 18]（充足されたパス） クエリ-回答木中のある頂点からある子孫の頂点へのパスは，セッション i のすべての証明者（検証者）メッセージの辺（頂点）を含むとき，セッション i を充足するという．パス中に最初の検証者メッセージが現れるすべてのセッションを充足するとき，そのパスは充足されるという．

[定義 19]（μ-good） クエリ-回答木の部分木が，μ 個のセッションを含むある再帰ブロック中の最初のメインセッションの最初のメッセージに対応するルートを持ち，そのルートから始まる充足されたパスを含むとき，μ-good であると呼ぶ．

[補題 5 の証明] ある定数 c が存在して，十分に大きな k に対して，$t_S(k)\leq k^c$ とする．$\mathrm{EXEC}_x(\sigma,g,h)$ 中のブロック接頭語がいずれも潜在的有用でないような三つ組 (σ,g,h) が存在すると仮定し，$S^{V^*}(x)$ が k^c 回より多くクエリを行うことを示す．

$W(\mu)$ を μ-good 部分木のサイズとする．後で示す補題 6 より，いかなる μ-good 部分木も以下を満たす：

$$W(\mu)\geq\begin{cases}1, & \mu\leq k,\\ r^{c+1}\cdot W(\frac{\mu-k}{r}), & \mu>k.\end{cases}$$

これより，有限個を除きすべての k に対して，$W(k^2)>k^c$ である．クエリ-回答木内の頂点はどれもシミュレータにより行われるクエリに対応しているので，シミュレータの実行時間が k^c で限定されるという仮定に矛盾する． □

[補題 4 の証明] d 番目ブロック接頭語が潜在的有用であることを $\mathsf{pot\text{-}use}_d(\sigma,g,h)$ と表す．補題 5 より，いかなる $(\sigma,g,h)\in \mathrm{AC}^k_x$ に対しても，潜在的有用ブロック接頭語が存在するので，

$$\Pr_{\sigma,g,h}[\forall d\forall i\ \neg\mathsf{useful}_{d,i}(\sigma,g,h)\wedge(\sigma,g,h)\in\mathrm{AC}^k_x]\leq\Pr_{\sigma,g,h}\left[\bigvee_{d=1}^{q_S(k)}(\mathsf{pot\text{-}use}_d(\sigma,g,h)\wedge\forall i\ \neg\mathsf{useful}_{d,i}(\sigma,g,h))\right].\tag{1}$$

$d\in\lfloor q_S(k)\rfloor$ において $\mathsf{pot\text{-}use}_d(\sigma,g,h)$ が真とする．定義 16 の条件（2）より，S の実行は，対応するブロックの終わりに到達する．つまり，再帰ブロック番号 $\ell^{\overline{bp}_d}$ の第 k メインセッションの $(r+1)$ 番目の証明者メッセージで終わっているクエリ $\overline{q}\in\mathrm{EXEC}_x(\sigma,g,h)$ が存在する．そのようなクエリのうち最初のものを $\overline{q}^{(\overline{bp}_d)}=\overline{q}^{(\overline{bp}_d)}(\sigma,g,h)$ とする．$\mathsf{accept}_{d,i}(\sigma,g,h)$ は，クエリ $\overline{q}^{(\overline{bp}_d)}$ がセッション $(\ell^{\overline{bp}_d},i)$ の受理対話を含むことを表すとする．このとき，すべての $i\in\mathcal{S}$ に対して $\mathsf{accept}_{d,i}(\sigma,g,h)$ が成立つサイズ $\frac{k^{1/2}}{4}$ の集合 $\mathcal{S}\subset[k]$ が存在する．よって，式 (1) は次のように上から抑えられる：

$$\Pr_{\sigma,g,h}\Big[\bigvee_{d=1}^{q_S(k)}\bigvee_{\substack{\mathcal{S}\subset[k]\\|\mathcal{S}|=\frac{k^{1/2}}{4}}}\mathsf{pot\text{-}use}_d(\sigma,g,h)\wedge(\forall i\in\mathcal{S}\ \neg\mathsf{useful}_{d,i}(\sigma,g,h)\wedge\mathsf{accept}_{d,i}(\sigma,g,h))\Big]\tag{2}$$

union bound により，式 (2) は次のように上から抑えられる：

$$\sum_{d=1}^{q_S(k)}\sum_{\substack{\mathcal{S}\subset[k]\\|\mathcal{S}|=\frac{k^{1/2}}{4}}}\Pr_{\sigma,g,h}[\mathsf{pot\text{-}use}_d(\sigma,g,h)\wedge(\forall i\in\mathcal{S}\ \neg\mathsf{useful}_{d,i}(\sigma,g,h)\wedge\mathsf{accept}_{d,i}(\sigma,g,h))]\tag{3}$$

主張 5 により，式 (3) は，次のように上から抑えられる：

$$\begin{aligned}&q_S(k)\cdot\binom{k}{\frac{k^{1/2}}{4}}\cdot\left(k^{-(1/2+1/4r)}\right)^{\frac{k^{1/2}}{4}}\\&<q_S(k)\cdot\left(\frac{4\cdot e\cdot k}{k^{1/2}}\right)^{\frac{k^{1/2}}{4}}\cdot\left(k^{-(1/2+1/4r)}\right)^{\frac{k^{1/2}}{4}}\\&=q_S(k)\cdot\left(\frac{4\cdot e}{k^{1/4r}}\right)^{\frac{k^{1/2}}{4}}<q_S(k)\cdot 2^{-\frac{k^{1/2}}{4}}.\end{aligned}\tag{4}$$

式 (4) は，

$$r<\frac{\log k}{4\cdot(3+\log e)},\tag{5}$$

ならば成立つが，これは定理 1 の仮定 $r(n)=o\left(\frac{\log n}{\log\log n}\right)=o\left(\frac{\log k}{\log\log k}\right)$ より十分大きな k に対して成立つ． □

3.6 補題 6 とその証明

[補題 6] $\mathrm{EXEC}_x(\sigma,g,h)$ 中に現れるすべてのブロック接頭語が潜在的有用でないとする．いかなる μ-good 部分木も，少なくとも r^{c+1} 個の $\frac{\mu-k}{r}$-good 部分木を含んでいる．

[定義 20]（T-クエリ） T をクエリ-回答木の任意の μ-good 部分木とする．T に対応する μ 個のセッションのうち，k 個のメインセッションが属する再帰ブロックを B_T とする．$\pi_{sn}(\overline{q})$ が B_T に属し，対応するパスがクエリ-回答木を下って T に属するノードで終わるようなクエリ $\overline{q}$ を T-クエリと呼ぶ．

[事実 1] $\mathrm{EXEC}_x(\sigma,g,h)$ 内のすべての T-クエリは同じブロック接頭語 $\overline{bp}_T$ を持つ．

[証明] 2 個の異なる T-クエリ $\overline{q}_1$ と $\overline{q}_2$ が存在し，$bp(\overline{q}_1)\neq bp(\overline{q}_2)$ と仮定すると，$\overline{q}_1$ と $\overline{q}_2$ は B_T 内の最初のメインセッションの最初のメッセージよりも前のメッセージにおいて異ならなければならない．そのためには，$\overline{q}_1$ と $\overline{q}_2$ に対応するパスが T のルートに達する前に分岐しなければならない．これは，これらが T 内のノードで終わらなければならないことに矛盾する． □

[主張 3] 補題 6 の仮定が成立っているとする．T を μ-good 部分木とする．ブロック接頭語 $\overline{bp}_T$ に対応する ip-相違クエリの個数は少なくとも r^{c+1} である．

[証明] $\ell = \ell^{(\overline{bp}_T)}$ をブロック接頭語 $\overline{bp}_T$ に対応する再帰ブロックの指標とする．補題 6 の仮定より，$\mathrm{EXEC}_x(\sigma, g, h)$ 内に現れるすべてのブロック接頭語は潜在的有用ではないので，$\overline{bp}_T$ も潜在的有用ではない．定義 16 の 2 つの条件の少なくともいずれかが破れていなければならない：

（1） ブロック接頭語 $\overline{bp}_T$ に対応する ip-相違クエリの個数は少なくとも r^{c+1} である．

（2） $\mathrm{EXEC}_x(\sigma, g, h)$ 内には $\mathrm{p}_{r+1}^{(\ell,k)}$ メッセージで終わるクエリは存在しない．

T は μ-good 部分木なので，充足されたパスを含む．そのようなパスは，ルートから始まり最初の検証者メッセージがパスに含まれるすべてのセッションを充足する．部分木 T のルートから始まる充足されたパスはいずれも B_T 内ですべてのメインセッションを充足する．従って，部分木 T は，T のルートから始まりセッション番号 (ℓ, k) の最後の証明者メッセージ（$\mathrm{p}_{r+1}^{(\ell,k)}$ メッセージ）でラベル付けられた辺で終わるパスを含んでいる．よって，$\mathrm{EXEC}_x(\sigma, g, h)$ は $\mathrm{p}_{r+1}^{(\ell,k)}$ メッセージで終わるクエリ $\overline{q}$ を含んでいるので，上の条件 (2) は成り立たない．従って，条件 (1) が成り立たなければならない． □

[主張 4] T を μ-good 部分木とする．ブロック接頭語 $\overline{bp}_T$ に対応する ip-相違クエリのいかなる対に対しても，部分木 T は 2 つの互いに素な $\frac{\mu-k}{r}$-good 部分木を含んでいる．

[定義 21]（反復接尾語） クエリ $\overline{q}$ ($j = \pi_{msg}(\overline{q}) > 1$ を満たす）の反復接尾語は，クエリ $\overline{q}$ の反復接頭語の終わりから始まる $\overline{q}$ の接尾語である．$is(\overline{q})$ と表記する．

[表記 1] $\mathcal{P}(\overline{q})$ は，クエリ-回答木の中のクエリ $\overline{q}$ に対応するパスを表す．$\mathcal{P}(ip(\overline{q}))$ は，$\overline{q}$ の反復接頭語 $ip(\overline{q})$ に対応する $\mathcal{P}(\overline{q})$ の部分木を表し，全体の木のルートから始まり，ある $\mathrm{p}_{j-1}^{(\ell,k)}$ メッセージで終わる．$\mathcal{P}(is(\overline{q}))$ は，$\overline{q}$ の反復接尾語 $is(\overline{q})$ に対応する $\mathcal{P}(\overline{q})$ の部分木を表し，ある $\mathrm{p}_{j-1}^{(\ell,k)}$ メッセージから始まり，ある $\mathrm{v}_j^{(\ell,i)}$ で終わる．$\mathcal{P}(\overline{q})$ は，$\mathcal{P}(ip(\overline{q}))$ と $\mathcal{P}(is(\overline{q}))$ を連接して得られる．

[事実 2] すべてのクエリ $\overline{q}$ に対して，部分パス $\mathcal{P}(is(\overline{q}))$ は充足される．さらに，

（1） 部分パス $\mathcal{P}(is(\overline{q}))$ は 1 レベル下位の再帰呼出しの中の $\frac{\mu-k}{r}$ 個のセッションのすべてを充足する．

（2） $\overline{q}$ がブロック接頭語 $\overline{bp}_T$ に対応するならば，部分パス $\mathcal{P}(is(\overline{q}))$ は T に含まれている．

[証明] $(\ell, i) = \pi_{sn}(\overline{q})$，$j = \pi_{msg}(\overline{q})$ とする．スケジューリングの性質により，部分パス $\mathcal{P}(is(\overline{q}))$ が始まる頂点は，再帰ブロック番号 ℓ によって行われる $(j-1)$ 番目の再帰呼出しに含まれるすべてのセッションの最初のメッセージよりも先にある．また，クエリ $\overline{q}$ は $\mathrm{v}_j^{(\ell,i)}$ メッセージにより回答されるので，部分パス $\mathcal{P}(is(\overline{q}))$ は，上のセッションの各々に対して最初と最後のメッセージを含んでいる．つまり，これらのセッションはすべて $\mathcal{P}(is(\overline{q}))$ により充足される．部分パス $\mathcal{P}(is(\overline{q}))$ に沿って最初のメッセージが現れるセッションは，それらだけであるので，$\mathcal{P}(is(\overline{q}))$ は充足される．

$\overline{q}$ がブロック接頭語 $\overline{bp}_T$ に対応するとき，部分木 $\mathcal{P}(is(\overline{q}))$ は，その開始点（$\mathrm{p}_{j-1}^{(\ell,k)}$）と終了点（$\mathrm{v}_j^{(\ell,i)}$）がともに T に含まれるので，部分木 T 内に含まれる． □

[事実 3] $\overline{q}_1$ と $\overline{q}_2$ は 2 つの ip-相違クエリとする．部分パス $\mathcal{P}(is(\overline{q}_1))$ と $\mathcal{P}(is(\overline{q}_2))$ は互いに素である．

[証明] $\overline{q}_1$ と $\overline{q}_2$ を 2 つの ip-相違クエリとし，$(\ell_1, i_1) = \pi_{sn}(\overline{q}_1)$ と $(\ell_2, i_2) = \pi_{sn}(\overline{q}_2)$，$j_1 = \pi_{msg}(\overline{q}_1)$ と $j_2 = \pi_{msg}(\overline{q}_2)$ とする．ip-相違の仮定（$ip(\overline{q}_1) \neq ip(\overline{q}_2)$）より，パス $\mathcal{P}(ip(\overline{q}_1))$ と $\mathcal{P}(ip(\overline{q}_2))$ は異なる．これは，以下の 2 つの場合に区別できる：

（1） $\mathcal{P}(ip(\overline{q}_1))$ が $\mathcal{P}(ip(\overline{q}_2))$ から分岐する：このとき，$\mathcal{P}(ip(\overline{q}_1))$ と $\mathcal{P}(ip(\overline{q}_2))$ の終点はクエリ-回答木の異なる部分木に属する．反復接尾語の始点は対応する反復接頭語の終点なので，$\mathcal{P}(is(\overline{q}_1))$ と $\mathcal{P}(is(\overline{q}_2))$ は互いに素である．

（2） $\mathcal{P}(ip(\overline{q}_1))$ は $\mathcal{P}(ip(\overline{q}_2))$ の接頭語である：$\mathcal{P}(ip(\overline{q}_1))$ と $\mathcal{P}(ip(\overline{q}_2))$ は両方とも $\mathrm{v}_{j_1-1}^{(\ell_1,k)}$ 頂点に達し，$\mathcal{P}(if(\overline{q}_2))$ はさらに木を下り，$\mathrm{v}_{j_2-1}^{(\ell_1,k)}$ 頂点まで達する．$\ell_1 = \ell_2$ かつ $j_1 = j_2$ のときは，$ip(\overline{q}_1)$ は $ip(\overline{q}_2)$ に等しいので，仮定に反する。よって，ℓ_1 が ℓ_2 より小さいか，あるいは，j_1 が j_2 より小さいかである．$\mathcal{P}(ip(\overline{q}_1))$ は $\mathrm{p}_{j_1}^{(\ell_1,k)}$ 頂点に始まり $\mathrm{v}_{j_1}^{(\ell_1,i_1)}$ 頂点に終わり，$\mathcal{P}(ip(\overline{q}_2))$ は $\mathrm{p}_{j_2}^{(\ell_2,k)}$ 頂点に始まり $\mathrm{v}_{j_2}^{(\ell_2,i_2)}$ 頂点に終わるので，$\mathcal{P}(is(\overline{q}_1))$ の終点は $\mathcal{P}(is(\overline{q}_2))$ の始点よりも前にある．つまり，$\mathcal{P}(is(\overline{q}_1))$ と $\mathcal{P}(is(\overline{q}_2))$ は互いに素である．

□

[主張 4 の証明] ブロック接頭語 $\overline{bp}_T$ に対応する 2 個の ip-相違クエリ $\overline{q}_1$ と $\overline{q}_2$ とすると，事実 2 (2) より，反復接尾語 $\mathcal{P}(is(\overline{q}_1))$ と $\mathcal{P}(is(\overline{q}_2))$ は，それぞれの始点をルートとする部分木 T_1 と T_2 に含まれる．事実 3 より，$\mathcal{P}(is(\overline{q}_1))$ と $\mathcal{P}(is(\overline{q}_2))$ は互いに素であるので，T_1 と T_2 も互いに素である．事実 2 (1) より，反復接尾語 $\mathcal{P}(is(\overline{q}_1))$ と $\mathcal{P}(is(\overline{q}_2))$ は，1 レベル下位の呼出しに属するすべてのセッションのすべてのメッセージを含んでいるので，$\frac{\mu-k}{r}$-good である． □

[補題 6 の証明] 主張 3 より，ブロック接頭語 $\overline{bp}_T$ に対応する相異なるクエリの個数は r^{c+1} より大きい．主張 4 より，ブロック接頭語 $\overline{bp}_T$ に対応する異なるクエリのいかなる対に対しても，部分木 T は，2 つの互いに素な $\frac{\mu-k}{r}$-good 部分木を含んでいるので，T は合わせて少なくとも r^{c+1} 個の互いに素な $\frac{\mu-k}{r}$-good 部分木を含んでいる． □

3.7 主張 5 とその証明

[主張 5] すべての $\sigma \in \{0,1\}^*$，すべての $h \in H$，すべての $d \in [q_S(k)]$，$|S| > r$ なるすべての集合 $S \subset [k]$ に対して，

$$\Pr_g[\mathsf{pot\text{-}use}_d(\sigma, g, h) \wedge \left(\forall i \in S\ \neg\mathsf{useful}_{d,i}(\sigma, g, h) \wedge \mathsf{accept}_{d,i}(\sigma, g, h)\right)] < \left(k^{-(1/2+1/4r)}\right)^{|S|}.$$

[定義 22] $x \in \{0,1\}^*$，$\sigma \in \{0,1\}^*$，$h \in H$，$d \in [k]$ を固定する．$\mathrm{EXEC}_x(\sigma, h, g)$ 中の d 番目ブロック接頭語を $\overline{bp}_d = \overline{bp}_d(g)$ と，対応する再帰ブロックの指標を $\ell^{(\overline{bp}_d)}$ と表記する．G から一様に選択された g を，G から一様に選択された 2 つの

$t_S(k)$-wise 独立ハッシュ関数 g_1 と g_2 を用いて，以下の条件を満たす g' の集合中に一様分布する $g^{(g_1,g_2)} = g^{(\sigma,h,d,g_1,g_2)}$ によって表す：$\overline{bp}_d$ に到達する前に生じた入力 α に適用された g' の値は $g_1(\alpha)$ に等しく，$\overline{bp}_d$ に到達した後に生じた入力 α に適用された g' の値は $g_2(\alpha)$ に等しい．

[命題 1] g_1 と g_2 が一様分布するとき，$g^{(g_1,g_2)}$ も一様分布するので，

$$\begin{aligned}&\Pr_g[\mathsf{pot\text{-}use}_d(\sigma,g,h) \wedge \\ &\qquad (\forall i\in S\ \neg\mathsf{useful}_{d,i}(\sigma,g,h) \wedge \mathsf{accept}_{d,i}(\sigma,g,h))] \\ &= \Pr_{g_1,g_2}[\mathsf{pot\text{-}use}_d(\sigma,g^{(g_1,g_2)},h) \wedge \\ &(\forall i\in S\ \neg\mathsf{useful}_{d,i}(\sigma,g^{(g_1,g_2)},h) \wedge \mathsf{accept}_{d,i}(\sigma,g^{(g_1,g_2)},h))].\end{aligned} \tag{6}$$

[事実 4] $\mathsf{pot\text{-}use}_d(\sigma,g,h) \wedge (\forall i\in S\ \neg\mathsf{useful}_{d,i}(\sigma,g,h) \wedge \mathsf{accept}_{d,i}(\sigma,g,h))$ が成り立つとき，

（1） ブロック接頭語 $\overline{bp}_d$ に対応する相異なる反復接頭語の個数は，高々 r^{c+1} である．

（2） すべての $j \in [r+1]\backslash\{1\}$ に対して，ひとつの反復接頭語 $\overline{ip}_j$ が存在して，すべての $i \in S$ に対して，$g_2(i,\overline{ip}_j) = 1$ である．

（3） すべての $i \in S$ に対して，ひとつの反復接頭語 $\overline{ip}^{(i)}$ が存在して，すべての $j \in [r+1]\backslash\{1\}$ に対して，$\overline{ip}^{(i)} \neq \overline{ip}_j$ かつ $g_2(i,\overline{ip}^{(i)}) = 1$ である．

[事実 4 の証明] （1）の証明は，ブロック接頭語 $\overline{bp}_d$ が潜在的有用であることを用いる．(2) の証明は，すべての $i \in S$ に対してクエリ $\overline{q}^{(\overline{bp}_d)}$ がセッション $(\ell^{(\overline{bp}_d,i)})$ に対する受理対話を含んでありことを用いる．(3) の証明は，すべての $i \in S$ に対してブロック接頭語 $\overline{bp}_d$ が i-有用でないことを用いる． □

[主張 5 の証明] $x \in \{0,1\}^*$，$\sigma \in \{0,1\}^*$，$h \in H$，$d \in [k]$ を固定する．$\mathrm{EXEC}_x(\sigma,h,g)$ 中の d 番目ブロック接頭語を $\overline{bp}_d = \overline{bp}_d(g)$ と，対応する再帰ブロックの指標を $\ell^{(\overline{bp}_d)}$ とする．上界を求めるべき確率は，$g \xleftarrow{R} G$ 上の確率である．しかし，ブロック接頭語 $\overline{bp}_d$ の内容は，g を選んだ後に決定される．まだ決定されていないブロック接頭語に対応する反復接頭語の上で一様に選択された g の振舞いを解析することは意味がない．そこで，以下の点に注目する：

（1） σ，h，d が固定されると，ブロック接頭語 $\overline{bp}_d$ の内容は，$\overline{bp}_d$ に最初に到達するよりも前に生じた入力に対する g の出力により，完全に決定される．

（2） ブロック接頭語 $\overline{bp}_d$ に対応するすべての反復接頭語は，$\overline{bp}_d$ に最初に到達した後に生ずる．

よって，σ，h，d を固定して，g の出力を以下のように区別し，すべての前者に対して，その後者の振舞いを解析する：

（1） $\mathrm{EXEC}_x(\sigma,g,h)$ 中の d 番目のブロック接頭語に到達する前に生じる g の出力

（2） $\overline{bp}_d$ に到達した後に生ずる g の出力

そこで，定義 22 の g_1 と g_2 を導入する．g_1 を固定して適切な反復接頭語上で一様に選択された g_2 の振舞いを解析する．いかなる g_1 の選択に対しても，g_2 の選択の上での式 (6) の確率が $(k^{-(1/2+1/4r)^{|S|}})$ によって上から抑えられることを示す．

σ，h，d，g_1 の選択によって決定されたブロック接頭語 $\overline{bp}_d$ を考え，$\mathrm{EXEC}_x(\sigma,g,h)$ 中の $\overline{bp}_d$ に対応する反復接頭語に注目する．g_2 は $t_S(k)$-wise 独立族からランダムに選択される．相異なる反復接頭語のいかなる対に対しても，g_2 の入力が異なるので，$t_S(k)$ 番目のクエリが S によって行われない限り，g_2 の出力は独立である．同様に，異なる $i,i' \in S$ の対に対しても，g_2 の入力が異なるので，出力は独立である．つまり，ブロック接頭語 $\overline{bp}_d$ に関連するすべての g_2 の出力は互いに独立である．一様に選択された g_2 が 1 を出力する確率は $k^{-1/2r}$ であるので，$\overline{bp}_d$ に対応する反復接頭語への g_2 の適用はすべて，確率 $k^{-1/2r}$ で成功する独立な実験と見なせる．

事実 4 (1) により，セッション $\{(\ell^{\overline{bp}_d},i)\}_{i\in S}$ に関連する g_2 の適用は高々 r^{c+1} 回の実験の系列と見なせる．その個々の実験は，確率 $k^{-1/2r}$ で成功する $|S|$ 個の独立な部分実験から構成される．事実 4 (2) により，上の実験のうち厳密に r 個が十分に（部分実験がすべて）成功する．しかし，事実 4 (3) により，すべての $i \in S$ に対して，それ以外にも成功する部分実験が存在する．部分実験が成功する確率が $k^{-1/2r}$ であることを使うと，ある実験が十分に成功する確率は $(k^{-1/2r})^{|S|}$ に等しい．式 (6) は次の 2 つの事象の生起確率により上から抑えられる：

（1） 各々が確率 $k^{-1/2r}$ で成功する高々 r^{c+1} 個の実験の系列において，厳密に r 個の成功する実験が存在する．

（2） 各々が確率 $k^{-1/2r}$ で成功する高々 $r^{c+1}-r$ 個の実験からなる $|S|$ 個の系列のすべてに対して，少なくとも 1 個の成功する実験が存在する．

$$\begin{aligned}&\binom{r^{c+1}}{r}\cdot\left((k^{-1/2r})^{|S|}\right)^r\cdot\left(1-(1-k^{-1/2r})^{r^{c+1}-r}\right)^{|S|}, \\ &< (r^{c+1})^r\cdot(k^{-1/2r})^{r\cdot|S|}\cdot(r^{c+1}\cdot k^{-1/2r})^{|S|}, \qquad (7) \\ &< (r^{c+1})^{r+|S|}\cdot(k^{-1/2r})^{r\cdot|S|+|S|}, \\ &= (r^{c+1})^{r+|S|}\cdot(k^{-1/4r})^{|S|}\cdot(k^{-(1/2+1/4r)})^{|S|}, \\ &< (k^{-(1/2+1/4r)})^{|S|}. \qquad (8)\end{aligned}$$

式 (7) は，

$$r^{c+1} - r = o(k^{1/2r}), \tag{9}$$

ならば成立つが，これは $r = o(\frac{\log k}{\log\log k})$ ならば満たされる．さらに，式 (8) は，

$$(r^{c+1})^{r+|S|}\cdot(k^{-1/4r})^{|S|} < 1, \tag{10}$$

ならば成立つが，これは $|S| > r$ かつ $r = o(\frac{\log k}{\log\log k})$ ならば満たされる．こうして，

$$\begin{aligned}&\Pr_g[\mathsf{pot\text{-}use}_d(\sigma,g,h) \wedge \\ &\quad (\forall i\in S\ \neg\mathsf{useful}_{d,i}(\sigma,g,h) \wedge \mathsf{accept}_{d,i}(\sigma,g,h))] \\ &<(k^{-(1/2+1/4r)})^{|S|}.\end{aligned}$$

□

4. 限定並行の下界

[定理 2] $m \in Poly(k)$ とする．非自明言語に対する m-cBBZKIP プロトコルのラウンド数 r は下界 $r = o(\frac{\log m}{\log \log m})$ を持つ．

[証明] $n = m \times poly(k)$ とし，$m = k^2$ とする．図 1 に示すスケジュールを考える．m 個のセッションを処理する再帰ブロック $\mathcal{R}(m)$ が逐次的に実行される．このスケジュールは m-限定並行性を満たしている．$\mathcal{R}(m)$ は，定理 1 の証明に用いたものと同じである．したがって，ラウンド数 r は下界 $r = o(\frac{\log m}{\log \log m})$ を持つ． □

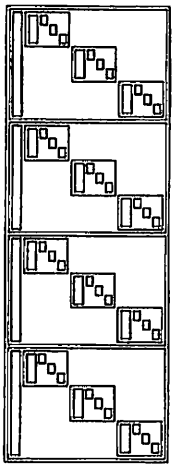

図 1 m-限定並行の場合のスケジュール：再帰ブロック $\mathcal{R}(m)$ が逐次的に処理される．$\mathcal{R}(m)$ の内部は，再帰ブロックが再帰的に呼出される．

Fig. 1 A schedule for m-bounded concurrency

5. 考　　察

今回得た結果と合わせて，plain model における m-cBBZKIP プロトコルのラウンド数の下界（プロトコルが存在し得ない十分条件）と上界（プロトコルが存在し得る十分条件）に関する知見をまとめ考察する．

同じ種類のプロトコルのみを合成する場合を自己合成，異なる種類のプロトコルを合成する場合を一般合成と呼ぶ．今回得た下界は，自己合成の場合の m-cBBZKIP のラウンド数の下界 $r_{\mathrm{self},m} = o\left(\frac{\log m}{\log \log m}\right)$ である．一般合成は，自己合成を特別な場合として含むので，一般合成の場合の m-cBBZKIP のラウンド数の下界 $r_{\mathrm{general},m}$ は，$r_{\mathrm{self},m} \leqq r_{\mathrm{general},m}$ を満たす．

一方，上界に関しては，自己合成の場合 [13] と妥当な制約の下での一般合成の場合 [14] のそれぞれに対して，上界 $\bar{r}_{\mathrm{self},m} = \omega(\log m)$ と $\bar{r}_{\mathrm{general},m} = \omega(\log m)$ を得ている．この場合も，一般には，$\bar{r}_{\mathrm{self},m} \leqq \bar{r}_{\mathrm{general},m}$ だが，得られている上界で両者の漸近的オーダは一致している．

当然だが，$r_{\mathrm{general},m} \leqq \bar{r}_{\mathrm{general},m}$ かつ $r_{\mathrm{self},m} \leqq \bar{r}_{\mathrm{self},m}$ である．

以上をまとめると，漸近的オーダによる関係は，

$$o\left(\frac{\log m}{\log \log m}\right) = r_{\mathrm{self},m} \leqq r_{\mathrm{general},m} < \bar{r}_{\mathrm{self},m} = \bar{r}_{\mathrm{general},m} = \omega(\log m),$$

となる．$r_{\mathrm{general},m}$ と $\bar{r}_{\mathrm{self},m}$ の大小関係は，一般には，何も言えないが，ここでは，$\bar{r}_{\mathrm{self},m} = \bar{r}_{\mathrm{general},m}$ から不等号を入れた．一般合成と自己合成のいずれの場合も，上界と下界が $\omega(\log m)$ と $o\left(\frac{\log m}{\log \log m}\right)$ の間にあることから，漸近的ラウンド数は，ほぼ $\log m$ オーダで最適である．

6. ま と め

プレインモデルにおける m-限定並行ブラックボックス零知識対話証明プロトコルのラウンド数の下界 $o\left(\frac{\log m}{\log \log m}\right)$ を得た．先に得た，自己合成および一般合成に対するラウンド数上界 $\omega(\log m)$ と合わせて考えると，漸近的ラウンド数は，ほぼ $\log m$ オーダで最適である．

文　　献

[1] O. Goldreich and Y. Oren: "Definitions and Properties of Zero-Knowledge Proof Systems", Journal of Cryptology, **7**, 1, pp. 1–32 (1994).

[2] O. Goldreich and A. Kahan: "How To Construct Constant-Round Zero-Knowledge Proof Systems for NP", Journal of Cryptology, **9**, 3, pp. 167–189 (1996).

[3] O. Goldreich and H. Krawczyk: "On the Composition of Zero-Knowledge Proof Systems", SIAM Journal on Computing, **25**, 1, pp. 169–192 (1996).

[4] C. Dwork, M. Naor and A. Sahai: "Concurrent Zero-Knowledge", STOC'98, ACM, pp. 409–418 (1998).

[5] J. Kilian, E. Petrank and C. Rackoff: "Lower Bounds for Zero Knowledge on the Internet", FOCS'98, IEEE, pp. 484–492 (1998).

[6] R. Richardson and J. Kilian: "On the Concurrent Composition of Zero-Knowledge Proofs", EUROCRYPT'99, Vol. 1592 of LNCS, Springer-Verlag, pp. 415–431 (1999).

[7] A. Rosen: "A Note on the Round-Complexity of Concurrent Zero-Knowledge", CRYPTO 2000, Vol. 1880 of LNCS, Springer-Verlag, pp. 451–468 (2000).

[8] J. Kilian and E. Petrank: "Concurrent and Resettable Zero-Knowledge in Poly-logarithmic Rounds", STOC'01, ACM, pp. 560–569 (2001).

[9] R. Canetti, J. Kilian, E. Petrank and A. Rosen: "Black-Box Concurrent Zero-Knowledge Requires $\tilde{\Omega}(\log n)$ Rounds", STOC'01, ACM, pp. 570–579 (2001).

[10] M. Prabhakaran and A. Sahai: "On the Concurrent Zero Knowledge Proofs with Logarithmic Round-Complexity", ECCC 2002 (2002).

[11] M. Prabhakaran, A. Rosen and A. Sahai: "Concurrent Zero-Knowledge With Logarithmic Round Complexity", FOCS 2002, IEEE, pp. 366–375 (2002).

[12] Y. Lindell: "Lower Bounds and Impossibility Results for Concurrent Self Composition", Cryptology ePrint Archive Report 2004/045 http://eprint.iacr.org (2004).

[13] H. Muratani: "Improved Round Complexity of Bounded Concurrent Zero-Knowledge", SCIS 2005, Vol. II, pp. 811–816 (2005).

[14] H. Muratani: "General Composition of a Bounded Concurrent Black-Box Zero-Knowledge Protocol", IEICE Technical Reprot, No. ISEC2006-7, pp. 45–52 (2006).