Non-overlapping template matching test を用いたテンプレートの同定の改善について

神奈川工科大　竹田　裕一　　中央大・理工　藤井　光昭
中央大・理工　渡邉　則生　　中央大・理工　鎌倉　稔成

現在まで統計関連学会等で、改良型 Non-overlapping template matching test を用いて、帰無仮説である 0 と 1 が $\frac{1}{2}$ の確率で独立に出現する数列より、多く含まれる未知のビット数を持つ 0 と 1 からなるあるパターン（以下これをテンプレートと呼ぶ）を同定する方法を提案した。Non-overlapping template matching test は、特定のパターンが 0-1 数列の中に含まれている個数を数え、帰無仮説のもとでの分布と比較し、分布に差があるかどうかを調べる検定である。この検定における対立仮説は、特定のパターンであるテンプレートが帰無仮説のもとより多く含まれることである。さらに、テンプレートの同定を行うことができれば、暗号理論の観点では非常に有用なものである。しかし、テンプレートはビット数・型ともに未知であり、考え得るすべてのパターンに対して検定を行うことは妥当な方法とは言えない。そのため、まずは短いビット数（例えば 3〜4 ビット程度）の全てのパターンで検定を行い、そこで棄却されたパターンを組み合わせることによって、より長いビット数のパターンを作り、検定を行って p 値を比較することによってテンプレートを同定する方法を過去に提案した。提案した手法はシミュレーション実験で多くの場合テンプレートの特定に成功する割合が高かったが、$00\cdots01$ のような一部の型で非常に悪い結果であった。

本発表では、テンプレート同定方法の改善案として、次のような方法を提案する。

- 初期設定：検定を行う短いパターンの初期ビット数 m^* と有意水準 α を決め、さらに B^0 を空集合とする。
- 第 1 段階：m^* ビットの 2^{m^*} 個ある全てのパターン（並び順）に対して検定を行い、p 値を求める。第 1 段階ではすべてのパターンを残し、その集合を B^1 とする。
- 第 k 段階 $(k \geqq 2)$：第 $k-1$ 段階で残されたの集合 B^{k-1} を組み合わせてできるパターンを作成し、作成されたパターンに対して検定を行い、p 値が α 以下であれば、第 $k+1$ 段階で使用するパターンの集合 B^k に入れる。p 値が α 以上であっても、組み合わせのもとになった 2 つのパターンの p 値よりも小さくなっていれば B^k に入れる。
- 特　　定：ある k_0 $(k_0 \geqq 2)$ について B^{k_0} が空集合になった場合、B^{k_0-1} と B^{k_0-2} の集合に含まれるパターンの p 値を比較し、最小値をとるパターンの集合を「特定したパターン」とする。
- 停　　止：必要であれば停止する段階 k_{max} を事前に定めておき、$B^{k_{max}}$ が空集合で無かった場合 $B^{k_{max}}$ と $B^{k_{max}-1}$ の集合に含まれるパターンの p 値を比較し、最小値をとるパターンの集合を「特定したパターン」とする。

上記の提案手法でシミュレーション実験を行ったところ、成功割合が悪い型の場合について、改善が見られた。シミュレーション結果などの詳細については、当日報告する。