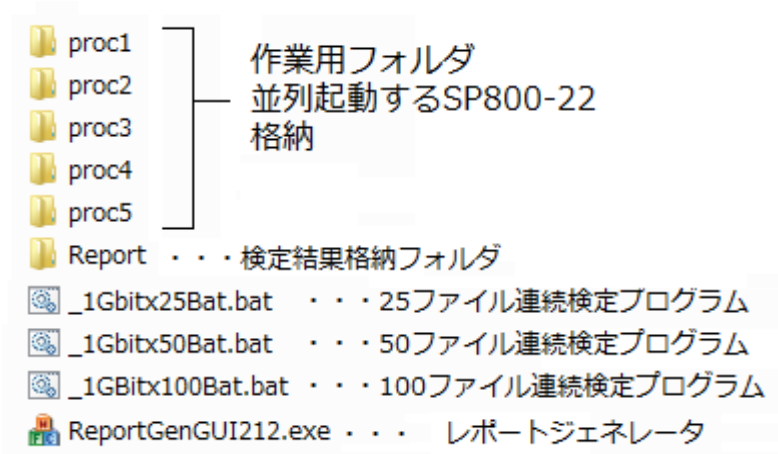


SP800-22 STS 2.1.2 x 100 説明書

1. 全体の構成



レポートジェネレータ以外は BAT ファイルで記述しています。

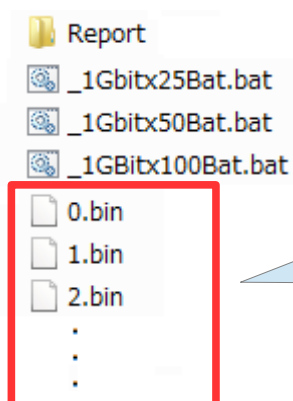
2. 100 ファイルの連続検定

2.1 掃除

Report **Report フォルダを消すか名前を変えてください。**

前回のレポートデータが残っていると結果がまざる場合があります。

2.2 乱数ファイルを用意



このように 0.bin ~ 99.bin までの
ファイルを同じフォルダにおいて
ください。

ファイル名は半角英数字です。

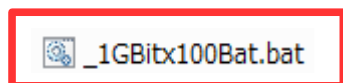
検定データは、「番号.bin」の規則に従い命名ください。

ファイルは **1Gbit(125MB)のバイナリファイル** で用意ください。

余裕を持ち少し大きめにすると安全です。

1K バイトを 1000 とするか 1024 とするか解釈が混乱があるので 1024 にすると安心です。

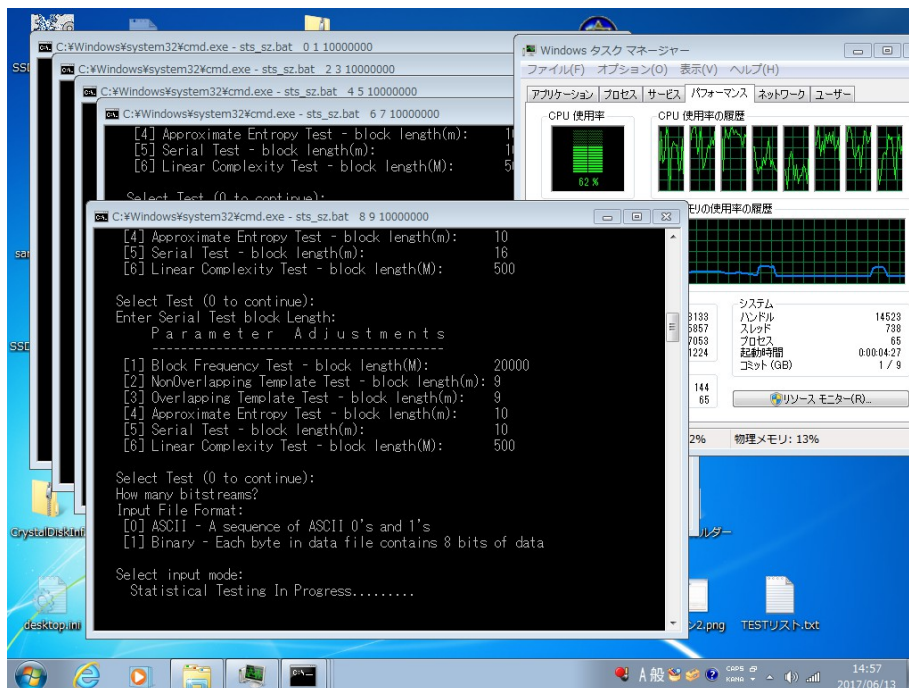
2.3 検定開始



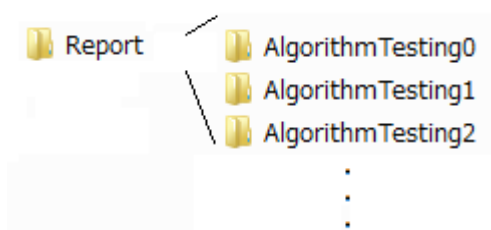
これをクリックすると
検定を開始します

次の画像のように5つの SP800-22 が並行起動して計算を始めます。

30 時間ほどお待ちください Zzzz...

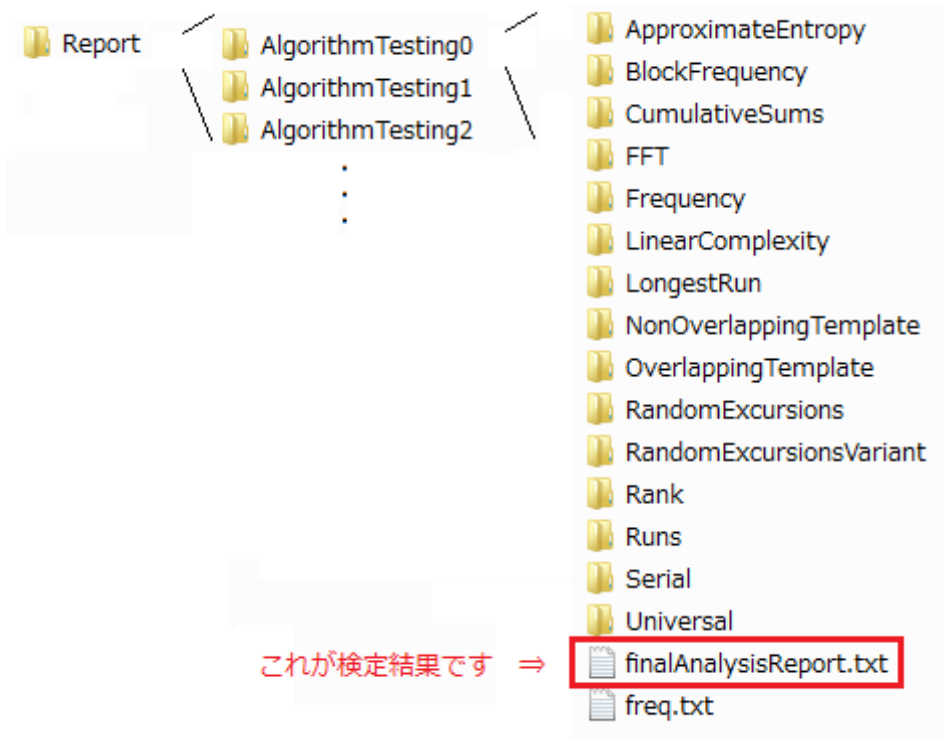


2.4 検定終了

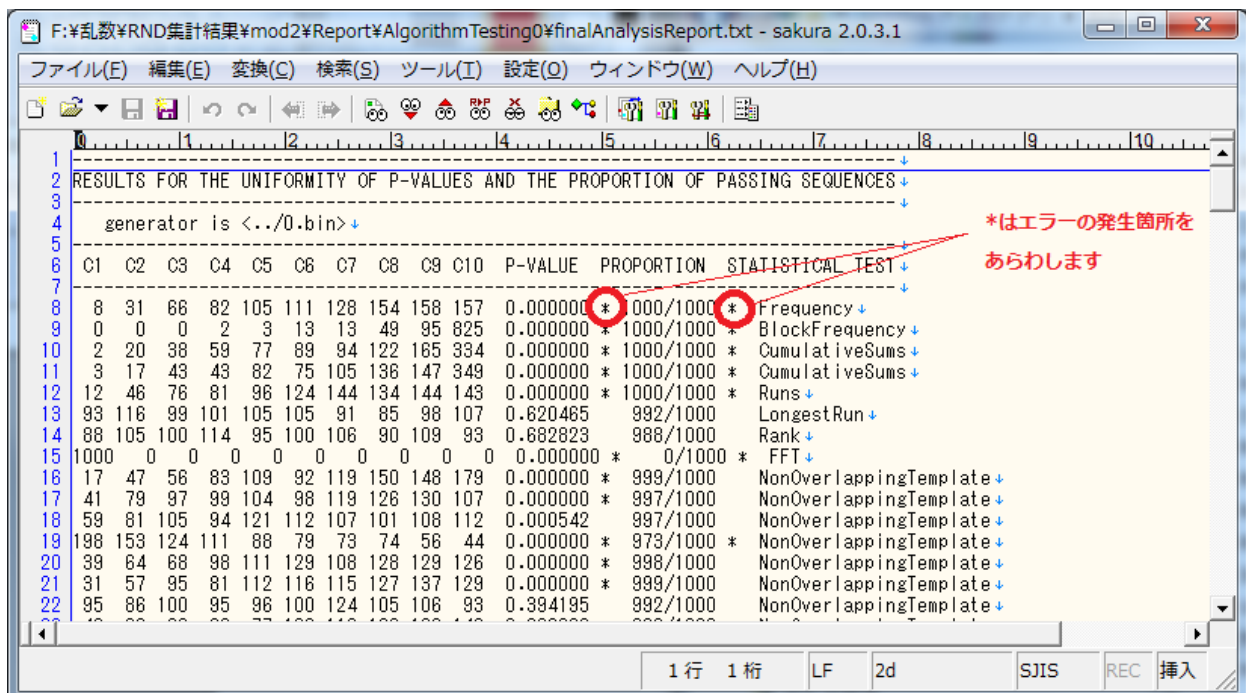


検定結果は Report フォルダの下にこのように出来
ます。

検定したファイルの数だけできます。



このファイルは Unix 系ファイルなので改行が LF コードです。LF に対応したエディタ/ワープロで開いてください。

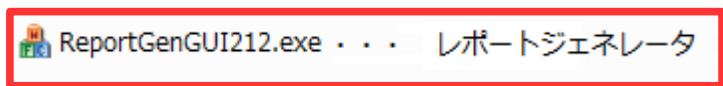


これはフリーウェアのサクラエディタで開いたところです。

3. レポートジェネレータ/自動分析プログラム



100本の検定結果を個別に確認していたら大変です。
ここではレポートジェネレータが活躍します。



これをクリックすると
自動分析開始



起動後処理に1~2分かかります。お待ちください。

さすがに検定結果100ファイル+各個別ファイル合計 3000 個の集計には
時間がかかります。



集計が終わるとレポート画面を出します。

3. 1. レポートの簡単な見方

このエラーが発生する場合、乱数の品質が悪いことを意味します。通常はゼロ、あるいは一見出るか否かを目安としてください。

8. NonOverlappingTemplate 補正エラー発生率=補正值 -4.96%
補正前 35.00% -- 39.96%の確率で発生するためこれを減算して補正

8 番のエラーはテストの性質上、約 40% の確率で発生が期待値のようです。

100 ファイルの検定を行い、ファイル合格率 80%以上、P-VAUE エラーがゼロあるいは1で合格と判断してください。

詳細表示...

エラー発生箇所の詳細を知りたい時はこのボタンを押してください。どの検定ファイルでエラーが出たかわかります。

Report.txt - メモ帳

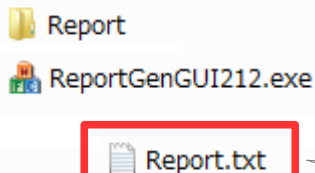
ファイル(E) 編集(E) 書式(O) 表示(V) ヘルプ(H)

=====
■ 本Reportの見方
1. 「1~g」の意味
各検定でエラーが出たことを「1~g」により示します。各検定の合格値は0.98以上です。
例外としてrandom-excursions(variant)テストは0.977944以上です。
2. 「8」「\$」の意味
テンプレートテストで、0.977944未満、0.96以上の項目に「8」を付けます。
0.96未満の時、「\$」を付けます。
このテストは148のテンプレートについてテストします。
このテストは正しい乱数においても1項目につき0.0028(百分率で0.28)と仮定します。
例) 148の項目のうち0.28の確率でエラーが発生すると判断します。
=====
Report¥AlgorithmTesting0¥finalAnalysisReport.txt p-value平均=0.513213 proportion平均=1.979938
Report¥AlgorithmTesting1¥finalAnalysisReport.txt 8 p-value平均=0.493826 proportion平均=1.979564
Report¥AlgorithmTesting2¥finalAnalysisReport.txt 88 p-value平均=0.491211 proportion平均=1.980074
Report¥AlgorithmTesting3¥finalAnalysisReport.txt 88 p-value平均=0.489728 proportion平均=1.980167
Report¥AlgorithmTesting4¥finalAnalysisReport.txt 8 p-value平均=0.439392 proportion平均=1.980067
Report¥AlgorithmTesting5¥finalAnalysisReport.txt 8 p-value平均=0.498967 proportion平均=1.980360
Report¥AlgorithmTesting6¥finalAnalysisReport.txt 8 p-value平均=0.495222 proportion平均=1.979487
Report¥AlgorithmTesting7¥finalAnalysisReport.txt 8 p-value平均=0.488449 proportion平均=1.980189
Report¥AlgorithmTesting8¥finalAnalysisReport.txt 8 p-value平均=0.461472 proportion平均=1.979385
Report¥AlgorithmTesting9¥finalAnalysisReport.txt 8 p-value平均=0.504700 proportion平均=1.980401
Report¥AlgorithmTesting10¥finalAnalysisReport.txt p-value平均=0.487073 proportion平均=1.979965
Report¥AlgorithmTesting11¥finalAnalysisReport.txt p-value平均=0.494041 proportion平均=1.979943
Report¥AlgorithmTesting12¥finalAnalysisReport.txt 5 p-value平均=0.459267 proportion平均=1.979787
Report¥AlgorithmTesting13¥finalAnalysisReport.txt 88 p-value平均=0.496808 proportion平均=1.978702
Report¥AlgorithmTesting14¥finalAnalysisReport.txt p-value平均=0.514056 proportion平均=1.979349
=====

8 はテンプレートエラーの発生を示します。テンプレートエラーは約40%の確率で出るのが期待値のようです。従い、このエラーは神経質になる必要はありません。

エラーの発生箇所には「1~g」のエラー番号が出ます。

テンプレートエラーで明らかな統計エラーが出た時は「8」のかわりに「\$」を表示します。



レポートジェネレータはカレントフォルダにある Report の中を自動検索して集計します。

詳細結果は同じフォルダに保存します。

4. 仕様

SP800-22 に指定するパラメータ

各パラメータは BAT ファイルで変更できます。詳細は BAT ファイル参照。

本ソフト出荷時は次の構成としています。

- 1000 本 × 1000,000 ビット長のストリームで処理
- Frequency の数値は 20000
- LOngeSt Run of Ones の数値は 10
- これ以外の設定は SP800-22 の規定値

5. 弊社への問い合わせ

http://dnki.co.jp/w2/2017/06/14/nist_sp800-22sts212/

本ソフトの配布希望の窓口にカスタム希望とメールをください。

連続検定とレポートジェネレータは弊社でも業務でひつようなので適時改良していきます。