計算機工学実験Ｂ 第１レポート

提出者　s153038　木戸 喜隆

提出日　2017 年 5 月 X 日

第１回 誤り制御符号 (1)：パリティ符号

1.1　実行結果

```
$./parity

情報語を10進数で入力してください(0?127　エンターのみで終了): 0
  入力値(10進数) = 0
  入力値( 2進数) = 0000000

  送信データ 0000000 0　(f6f5f4f3f2f1f0 p0)
  受信データ 0000010 0　(f6f5f4f3f2f1f0 p0)
  算出された検査ビット = 1

  伝送誤りが検出されました。

情報語を10進数で入力してください(0?127　エンターのみで終了): 0
  入力値(10進数) = 0
  入力値( 2進数) = 0000000

  送信データ 0000000 0　(f6f5f4f3f2f1f0 p0)
  受信データ 0000000 0　(f6f5f4f3f2f1f0 p0)
  算出された検査ビット = 0

  伝送誤りはありません。

情報語を10進数で入力してください(0?127　エンターのみで終了): 0
  入力値(10進数) = 0
  入力値( 2進数) = 0000000

  送信データ 0000000 0　(f6f5f4f3f2f1f0 p0)
  受信データ 0101000 0　(f6f5f4f3f2f1f0 p0)
  算出された検査ビット = 0

  伝送誤りはありません。
```

1.2　実行結果に対する考察

前節の実行結果より、1 ビット垂直パリティ符号ではデータに偶数個の１が含まれていると、誤りが検出できない可能性が存在することがわかる。また、奇数個の１が含まれていると、誤りが存在しないのに存在するという結果を出す可能性があると考えられる。

1.3　課題

(1)　今回の実験で作成したパリティ符号は、偶数パリティと奇数パリティのいずれかであるかを答えよ。

偶数パリティ送信データ 7 ビットとチェックビットを合わせた 8 ビットの排他的論理和の値が偶数０であることから偶数パリティであることがわかる。

(2)　１ビット水平パリティ符号について調査せよ。

ブロックごとに、BCC と呼ばれるパリティビット列を付加して、データ誤りが発生したかどうかを検出する。[1]

(3)　１ビット水平パリティ符号と１ビット垂直パリティ符号を組み合わせることにより、１ビットの誤りを訂正できることを示せ。

第2回 誤り制御符号 (2) : CRC 符号

2.1 実行結果

```
$./crc

情報語を10進数で入力してください(0?15  エンターのみで終了): 10
入力値(10進数) = 10
送信データ 1010 011  (f3f2f1f0 r2r1r0)
受信データ 0010 011  (f3f2f1f0 r2r1r0)
    シンドローム 1 0 1  (s2 s1 s0)
    誤り発生位置 = 6  (f3)
訂正データ 1010 011  (f3f2f1f0 r2r1r0)

情報語を10進数で入力してください(0?15  エンターのみで終了): 10
入力値(10進数) = 10
送信データ 1010 011  (f3f2f1f0 r2r1r0)
受信データ 1010 011  (f3f2f1f0 r2r1r0)
    シンドローム 0 0 0  (s2 s1 s0)
    誤りなし
訂正データ 1010 011  (f3f2f1f0 r2r1r0)

情報語を10進数で入力してください(0?15  エンターのみで終了): 10

入力値(10進数) = 10
送信データ 1010 011  (f3f2f1f0 r2r1r0)
受信データ 1110 011  (f3f2f1f0 r2r1r0)
    シンドローム 1 1 1  (s2 s1 s0)
    誤り発生位置 = 5  (f2)
訂正データ 1010 011  (f3f2f1f0 r2r1r0)
```

2.2 実行結果に対する考察

2.3 課題

(1) 生成多項式 $G(x) = x^3 + x + 1$ を用いて 4 ビットの情報語 $(0101)_2$ から 7 ビットの符号語を生成するとき、符号語が $G(x)$ で割り切れることを示せ.また, 符号語のどこか 1 ビットを変更した語を作成し, これが $G(x)$ で割り切れないことを示せ.

第３回 暗号化技術 (1) : 共通鍵暗号

3.1 実行結果

```
$
暗 号 化
Ifmmp Xpsme
AAA
bbb
BBB
aaa

復 号 化
Hello World
ZZZ
aaa
AAA
zzz
```

3.2 課題

(1) 今回の実験で使用したもの (鍵の値に応じて各文字の値をずらす) とは異なる共通鍵暗号方式のアルゴリズムを考え, 暗号化と復号化のアルゴリズムを図と文章を用いて説明せよ.

(2) (1) で示した共通鍵暗号方式の暗号化プログラム (original_encrypt.c) と復号化プログラム (original decrypt.c) を作成し,4.3 節で作成した caesar_sample.txt に対して暗号化と復号化を行った実行結果を示せ

参考文献

[1] 出典:http://mt-net.vis.ne.jp/ADFE_mail/0139.htm 徹底研究！情報処理試験より (検索日：2017/4/14)