The General Linear Group of $GF(2)^3$

Peter M. Maurer
Dept. of Computer Science
Baylor University
Waco, TX 76798-7356

These matrices are the non-singular 3x3 matrices over GF(2). They were generated by brute force. The basic algorithm generated all 3x3 GF(2) matrices by first enumerating all 3x3 matrices and then testing each one for singularity. The generator algorithm enumerated all numbers from 0 through 511, and then distributed the bits of the number into a 3x3 matrix of ones and zeros. To test for singularity, the various rows of the matrix were added in the following patterns. Row1 + Row2, Row1+Row3, Row2+Row3, Row1+Row2+Row3. Addition was accomplished by treating each row as a vector and doing a bitwise XOR on the three pairs of bits. If any test produced the zero vector, the matrix was immediately rejected, and the remaining tests were aborted.

The matrices are presented in the order generated. An ordinal number is printed above each matrix. Each matrix is followed by its inverse and its order. (The order of matrix M is the smallest positive integer k such that $M^k = I$, the identity matrix.) Thus the 10th generated matrix is:

10
001 010 7
100 101
011 100

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Its order is 7, and its inverse is:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

That is to say,

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I$$

The order and inverse were obtained using the following algorithm.

```
Matrix3 M(0,0,1  1,0,0  0,1,1);
Matrix3 I(1,0,0,  0,1,0  0,0,1);
Matrix3 Work,Inverse;
Work=M,Inverse=M;
int Order = 1;
while (Work != I)
{
    Inverse = Work;
    Work = Work * M;
    Order++;
}
```

Barring any typos, this code should work with the GF2Matrices package. Simply add the line #include <GF2Matrices.h> to the beginning of the program. The GF2Matrices package must be installed so the .h and .lib (or .a) files are accessible to the compiler. The program must be compiled with the GF2Matrices.lib library.

This code has been incorporated into the GF2Matrices package, so the following code simplification is possible.

```
Matrix3 M(0,0,1  1,0,0  0,1,1);
Matrix3 Inverse;
Inverse = M.Inverse( );
int Order = M.Order( );
```

The general linear group can also be generated by the GF2Matrices project using the following code.

```
Group3 G;

G.GenerateGLG( );
```

The individual matrices are accessible using the following code.

```
for (Matrix3 *Temp=G.GetFirstMatrix( ) ; Temp ; Temp = G.GetNextMatrix( ))
{
    // use *Temp, or Temp->Order( ) (etc.) to access matrices
}
```

The generation algorithm used by the GF2Matrices project is more sophisticated and faster than the technique described above. The following algorithm is used.

Each of the 8 possible rows is encoded as a 3-bit integer. No explicit enumeration of the rows is necessary. A 8-element array is used to mark rows as available or unavailable. Another 8

element array is used as a stack to contain all unavailable rows. The algorithm proceeds as follows.

```
Mark[0] = unavailable;
Push 0 on the stack;
for (int i =  0 ; i<8 ; i++)
{
  if (Mark[i] = available)
  {
    For all rows x in the stack
    {
      Mark[x ^ i] = unavailable;
      Push (x ^ i) on stack;
    }
    for (int j=0 ; j<8 ; j++)
    {
      If (Mark[j] = available)
      {
        For all rows x in the stack
        {
          Mark[x ^ j] = unavailable;
          Push (x ^ j) on stack;
        }
        for (int k=0 ; k<8 ; k++)
        {
          Generate a matrix with rows i,j,k;
        }
        Pop stack until j is popped.
      }
    }
    Pop stack until i is popped.
  }
}
```

This algorithm is based on the counting procedure for non-singular matrices over finite fields presented in Lidl & Niederreiter, “Finite Fields” Cambridge University Press, Jan 13, 1997.

1
001 001 2
010 010
100 100

2
001 101 3
010 010
101 100

3
001 011 4
010 010
110 100

4
001 111 3
010 010
111 100

5
001 001 4
011 110
100 100

6
001 101 3
011 110
101 100

7
001 111 7
011 110
110 100

8
001 011 7
011 110
111 100

9
001 010 3
100 001
010 100

10
001 010 7
100 101
011 100

11
001 010 7
100 011
110 100

12
001 010 4
100 111
111 100

13
001 110 7
101 001
010 100

14
001 110 4
101 101
011 100

15
001 110 3
101 111
110 100

16
001 110 7
101 011
111 100

17
001 011 7
110 001
010 100

18
001 111 7
110 101
011 100

19
001 001 4
110 011
100 100

20
001 101 3
110 111
101 100

21
001 111 4
111 001
010 100

22
001 011 3
111 101
011 100

23
001 001 2
111 111
100 100

24
001 101 3
111 011
101 100

25
010 001 3
001 100
100 010

26
010 011 7
001 100
101 010

27
010 101 7
001 100
110 010

28
010 111 4
001 100
111 010

29
010 001 7
011 100
100 110

30
010 111 7
011 100
101 110

31
010 101 4
011 100
110 110

32
010 011 3
011 100
111 110

33
010 010 2
100 100
001 001

34
010 010 4
100 100
011 101

35
010 010 4
100 100
101 011

36
010 010 2
100 100
111 111

37
010 011 4
101 100
001 001

38
010 111 7
101 100
011 101

39
010 001 7
101 100
100 011

40
010 101 3
101 100
110 111

41
010 110 3
110 100
001 001

42
010 110 3
110 100
011 101

43
010 110 3
110 100
101 111

44
010 110 3
110 100
111 011

45
010 111 3
111 100
001 001

46
010 011 7
111 100
011 101

47
010 001 4
111 100
100 111

48
010 101 7
111 100
110 011

49
011 001 7
001 110
100 010

50
011 011 4
001 110
101 010

51
011 111 3
001 110
110 010

52
011 101 7
001 110
111 010

53
011 001 4
010 010
100 110

54
011 111 3
010 010
101 110

55
011 011 2
010 010
110 110

56
011 101 3
010 010
111 110

57
011 010 4
100 101
001 001

58
011 010 7
100 001
010 101

59
011 010 7
100 111
101 011

60
011 010 3
100 011
110 111

61
011 011 2
101 101
001 001

62
011 111 3
101 001
010 101

63
011 001 3
101 111
100 011

64
011 101 4
101 011
111 111

65
011 111 3
110 101
001 001

66
011 011 4
110 001
010 101

67
011 001 7
110 011
100 111

68
011 101 7
110 111
111 011

69
011 110 3
111 101
001 001

70
011 110 7
111 001
010 101

71
011 110 7
111 011
101 111

72
011 110 4
111 111
110 011

73
100 100 2
001 001
010 010

74
100 100 3
001 011
011 010

75
100 100 4
001 101
110 010

76
100 100 3
001 111
111 010

77
100 100 1
010 010
001 001

78
100 100 2
010 010
011 011

79
100 100 2
010 010
101 101

80
100 100 2
010 010
111 111

81
100 100 2
011 011
001 001

82
100 100 3
011 001
010 011

83
100 100 4
011 111
101 101

84
100 100 3
011 101
110 111

85
100 100 4
101 001
010 110

86
100 100 3
101 111
011 110

87
100 100 2
101 101
110 110

88
100 100 3
101 011
111 110

89
100 100 2
110 110
001 001

90
100 100 4
110 110
011 111

91
100 100 2
110 110
101 101

92
100 100 4
110 110
111 011

93
100 100 2
111 111
001 001

94
100 100 3
111 001
010 111

95
100 100 4
111 011
101 101

96
100 100 3
111 101
110 011

97
101 110 4
001 001
010 010

98
101 110 3
001 011
011 010

99
101 110 7
001 111
110 010

100
101 110 7
001 101
111 010

101
101 101 2
010 010
001 001

102
101 111 4
010 010
011 011

103
101 001 3
010 010
100 101

104
101 011 3
010 010
110 111

105
101 101 2
011 011
001 001

106
101 111 3
011 001
010 011

107
101 001 3
011 111
100 101

108
101 011 4
011 101
111 111

109
101 010 7
100 001
010 110

110
101 010 7
100 111
011 110

111
101 010 4
100 011
110 110

112
101 010 3
100 101
111 110

113
101 101 4
110 111
001 001

114
101 011 7
110 001
010 111

115
101 001 3
110 011
100 101

116
101 111 7
110 101
111 011

117
101 101 4
111 110
001 001

118
101 011 7
111 110
011 111

119
101 001 3
111 110
100 101

120
101 111 7
111 110
110 011

121
110 101 4
001 001
010 010

122
110 111 3
001 011
011 010

123
110 001 7
001 101
100 010

124
110 011 7
001 111
101 010

125
110 110 2
010 010
001 001

126
110 110 2
010 010
011 011

127
110 110 4
010 010
101 111

128
110 110 4
010 010
111 101

129
110 111 4
011 011
001 001

130
110 101 3
011 001
010 011

131
110 001 7
011 101
100 111

132
110 011 7
011 111
111 101

133
110 010 3
100 110
001 001

134
110 010 3
100 110
011 111

135
110 010 3
100 110
101 011

136
110 010 3
100 110
111 101

137
110 011 3
101 111
001 001

138
110 101 7
101 001
010 111

139
110 001 4
101 101
100 011

140
110 111 7
101 011
111 101

141
110 101 7
111 001
010 110

142
110 011 4
111 111
011 110

143
110 001 3
111 101
100 110

144
110 111 7
111 011
101 110

145
111 111 2
001 001
010 010

146
111 101 3
001 011
011 010

147
111 001 4
001 111
100 010

148
111 011 3
001 101
101 010

149
111 111 2
010 010
001 001

150
111 101 4
010 010
011 011

151
111 001 3
010 010
100 111

152
111 011 3
010 010
110 101

153
111 110 4
011 011
001 001

154
111 110 3
011 001
010 011

155
111 110 7
011 101
101 111

156
111 110 7
011 111
110 101

157
111 010 3
100 111
001 001

158
111 010 4
100 001
010 111

159
111 010 7
100 101
101 011

160
111 010 7
100 011
110 101

161
111 011 3
101 110
001 001

162
111 101 7
101 110
011 111

163
111 001 7
101 110
100 011

164
111 111 4
101 110
110 101

165
111 011 3
110 001
010 110

166
111 101 7
110 111
011 110

167
111 001 7
110 011
100 110

168
111 111 4
110 101
101 110

The following is a list of the number of matrices of each order.

Order 1	1
Order 2	21
Order 3	56
Order 4	42
Order 5	0
Order 6	0
Order 7	48