**Characteristic $m$-Sequences**

By Michael Willett

**Abstract.** The initial $k$-tuple of the characteristic $m$-sequence associated with a primitive polynomial of degree $k$ over $GF(2)$ is given for $2 \leq k \leq 168$.

**Introduction.** In this note we take advantage of the list of primitive polynomials over $GF(2)$ published by Stahnke [1] to calculate a table of characteristic $m$-sequences. This author [2] has shown how a characteristic $m$-sequence may be used to generate a set of cycle representatives for any cyclic code with square-free parity check polynomial. Such cycle sets are important for determining the error-correcting capability of the cyclic code. In [2] cycle set members are formed by adding certain decimations of a characteristic $m$-sequence. This technique is computationally simpler than standard algorithms based on more complicated algebraic operations.

**Preliminaries.** Let $F$ be the binary field with two elements 0, 1. A polynomial $f(x) = x^k - a_1 x^{k-1} - \cdots - a_k \in F[x]$ is called primitive if a root of $f(x)$ in the extension field $K = GF(2^k)$ of $F$ generates the cyclic multiplicative group of $K$. There are $\varphi(2^k - 1)/k$ primitive polynomials of degree $k$, where $\varphi$ is Euler’s function. Assume that $f(x)$ is primitive and consider the linear recursion associated with $f(x)$ given by

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n, \quad n = 0, 1, 2, \ldots$$

(1)

Primitive polynomials are characterized by the fact that every nonzero solution to (1) over $F$ has minimum period $2^k - 1$. Therefore, all nonzero solutions to (1) are cyclic shifts of one another. Any such solution is called an $m$-sequence (or PN sequence). There exists a unique $m$-sequence $u = (u_0, u_1, \ldots)$ so that $u_n = u_{2n}$ for all $n$, called the characteristic $m$-sequence associated with $f(x)$.

**Algorithm.** The algorithm used to find the characteristic $m$-sequence below is easily adapted to finding such sequences over other prime fields. Treat the symbols $u_0, u_1, \ldots, u_{k-1}$ as unknowns. From recursion (1) formally calculate $u_k, u_{k+1}, \ldots, u_{2k-2}$, reducing each of these terms to a linear combination of the unknowns. Then solve the system of equations

$$u_n = u_{2n}, \quad n = 0, 1, \ldots, k-1,$$

(2)

for the unknowns. The unique nonzero solution will be the characteristic $m$-sequence associated with $f(x)$. The following table lists the initial $k$-tuple of the characteristic $m$-sequence associated with $f(x)$.
$m$-sequence associated with the primitive polynomial shown. Each polynomial is given by showing which powers of $x$ appear in $f(x)$; i.e., $f(x) = x^8 + x^6 + x^5 + x + 1$ is given by $8 \ 6 \ 5 \ 1 \ 0$. The notation $i^n$ will mean $n$ consecutive copies of the integer $i$.

The computations were performed on an IBM 370/165 computer. The sequences were verified by checking each sequence with its associated primitive polynomial in equation (2).

<table>
<thead>
<tr>
<th>Primitive polynomial</th>
<th>Characteristic $m$-sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>01</td>
</tr>
<tr>
<td>3</td>
<td>$10^2$</td>
</tr>
<tr>
<td>4</td>
<td>$0^31$</td>
</tr>
<tr>
<td>5</td>
<td>$10^210$</td>
</tr>
<tr>
<td>6</td>
<td>$0^51$</td>
</tr>
<tr>
<td>7</td>
<td>$10^6$</td>
</tr>
<tr>
<td>8</td>
<td>$0^3101^20$</td>
</tr>
<tr>
<td>9</td>
<td>$10^410^3$</td>
</tr>
<tr>
<td>10</td>
<td>$0^710^2$</td>
</tr>
<tr>
<td>11</td>
<td>$10^810$</td>
</tr>
<tr>
<td>12</td>
<td>$0^510^31^20$</td>
</tr>
<tr>
<td>13</td>
<td>$10^810^3$</td>
</tr>
<tr>
<td>14</td>
<td>$0^3101^30^21010$</td>
</tr>
<tr>
<td>15</td>
<td>$10^{14}$</td>
</tr>
<tr>
<td>16</td>
<td>$0^{11}1010^2$</td>
</tr>
<tr>
<td>17</td>
<td>$101010^310^51^20$</td>
</tr>
<tr>
<td>18</td>
<td>$0^{11}10^6$</td>
</tr>
<tr>
<td>19</td>
<td>$10^{12}10^5$</td>
</tr>
<tr>
<td>20</td>
<td>$0^{17}10^2$</td>
</tr>
<tr>
<td>21</td>
<td>$10^{18}10$</td>
</tr>
<tr>
<td>22</td>
<td>$0^{21}1$</td>
</tr>
<tr>
<td>23</td>
<td>$10^{22}$</td>
</tr>
<tr>
<td>24</td>
<td>$0^{21}101$</td>
</tr>
<tr>
<td>25</td>
<td>$10^{24}$</td>
</tr>
<tr>
<td>26</td>
<td>$0^{19}10^51$</td>
</tr>
<tr>
<td>27</td>
<td>$10^{18}10^7$</td>
</tr>
<tr>
<td>28</td>
<td>$0^{25}10^2$</td>
</tr>
<tr>
<td>29</td>
<td>$10^{26}10$</td>
</tr>
<tr>
<td>30</td>
<td>$0^{15}10^{14}$</td>
</tr>
<tr>
<td>31</td>
<td>$10^{30}$</td>
</tr>
<tr>
<td>32</td>
<td>$0^510^31^20^21010^150^410^310$</td>
</tr>
<tr>
<td>33</td>
<td>$10^{32}$</td>
</tr>
<tr>
<td>34</td>
<td>$0^{19}10^131$</td>
</tr>
<tr>
<td>35</td>
<td>$10^{32}10$</td>
</tr>
<tr>
<td>36</td>
<td>$0^{25}10^{10}$</td>
</tr>
<tr>
<td>37</td>
<td>$10^{24}101010^710$</td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
<table>
<thead>
<tr>
<th>Primitive polynomial</th>
<th>Characteristic $m$-sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>38 6 5 1 0</td>
<td>0331031</td>
</tr>
<tr>
<td>39 4 0</td>
<td>1034103</td>
</tr>
<tr>
<td>40 21 19 2 0</td>
<td>01910101610</td>
</tr>
<tr>
<td>41 3 0</td>
<td>1040</td>
</tr>
<tr>
<td>42 23 22 1 0</td>
<td>01910181201</td>
</tr>
<tr>
<td>43 6 5 1 0</td>
<td>1036105</td>
</tr>
<tr>
<td>44 27 26 1 0</td>
<td>017101612071</td>
</tr>
<tr>
<td>45 4 3 1 0</td>
<td>1040103</td>
</tr>
<tr>
<td>46 21 20 1 0</td>
<td>02510191</td>
</tr>
<tr>
<td>47 5 0</td>
<td>1046</td>
</tr>
<tr>
<td>48 28 27 1 0</td>
<td>021101912041</td>
</tr>
<tr>
<td>49 9 0</td>
<td>1048</td>
</tr>
<tr>
<td>50 27 26 1 0</td>
<td>02310221201</td>
</tr>
<tr>
<td>51 16 15 1 0</td>
<td>10341015</td>
</tr>
<tr>
<td>52 3 0</td>
<td>049102</td>
</tr>
<tr>
<td>53 16 15 1 0</td>
<td>10361015</td>
</tr>
<tr>
<td>54 37 36 1 0</td>
<td>017101612015102</td>
</tr>
<tr>
<td>55 24 0</td>
<td>10301023</td>
</tr>
<tr>
<td>56 22 21 1 0</td>
<td>03510191</td>
</tr>
<tr>
<td>57 7 0</td>
<td>1056</td>
</tr>
<tr>
<td>58 19 0</td>
<td>0391018</td>
</tr>
<tr>
<td>59 22 21 1 0</td>
<td>10361021</td>
</tr>
<tr>
<td>60 1 0</td>
<td>0591</td>
</tr>
<tr>
<td>61 16 15 1 0</td>
<td>10441015</td>
</tr>
<tr>
<td>62 57 56 1 0</td>
<td>0510412031010102101201012010210101401031302102101201010140</td>
</tr>
<tr>
<td>63 1 0</td>
<td>1062</td>
</tr>
<tr>
<td>64 4 3 1 0</td>
<td>061101</td>
</tr>
<tr>
<td>65 18 0</td>
<td>10461017</td>
</tr>
<tr>
<td>66 10 9 1 0</td>
<td>0571071</td>
</tr>
<tr>
<td>67 10 9 1 0</td>
<td>1056109</td>
</tr>
<tr>
<td>68 9 0</td>
<td>059108</td>
</tr>
<tr>
<td>69 29 27 2 0</td>
<td>106610</td>
</tr>
<tr>
<td>70 16 15 1 0</td>
<td>05510131</td>
</tr>
<tr>
<td>71 6 0</td>
<td>1064105</td>
</tr>
<tr>
<td>72 53 47 6 0</td>
<td>01910510121011106106105105102</td>
</tr>
<tr>
<td>73 25 0</td>
<td>1072</td>
</tr>
<tr>
<td>74 16 15 1 0</td>
<td>05910131</td>
</tr>
<tr>
<td>75 11 10 1 0</td>
<td>1064109</td>
</tr>
<tr>
<td>76 36 35 1 0</td>
<td>04110331</td>
</tr>
<tr>
<td>77 31 30 1 0</td>
<td>10461029</td>
</tr>
<tr>
<td>Primitive polynomial</td>
<td>Characteristic ( m )-sequences</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>78 20 19 1 0</td>
<td>( 0^{59}10^{17}1 )</td>
</tr>
<tr>
<td>79 9 0</td>
<td>( 10^{78} )</td>
</tr>
<tr>
<td>80 38 37 1 0</td>
<td>( 0^{43}10^{35}1 )</td>
</tr>
<tr>
<td>81 4 0</td>
<td>( 10^{6}610^{3} )</td>
</tr>
<tr>
<td>82 38 35 3 0</td>
<td>( 0^{47}10^{31}10^{2} )</td>
</tr>
<tr>
<td>83 46 45 1 0</td>
<td>( 10^{36}10^{36}1^{2}0^{7} )</td>
</tr>
<tr>
<td>84 13 0</td>
<td>( 0^{71}10^{12} )</td>
</tr>
<tr>
<td>85 28 27 1 0</td>
<td>( 10^{56}10^{27} )</td>
</tr>
<tr>
<td>86 13 12 1 0</td>
<td>( 0^{73}10^{11}1 )</td>
</tr>
<tr>
<td>87 13 0</td>
<td>( 10^{86} )</td>
</tr>
<tr>
<td>88 72 71 1 0</td>
<td>( 0^{17}10^{15}1^{2}0^{14}1010^{13}1^{4}0^{12}10^{3}101 )</td>
</tr>
<tr>
<td>89 38 0</td>
<td>( 10^{50}10^{37} )</td>
</tr>
<tr>
<td>90 19 18 1 0</td>
<td>( 0^{71}10^{17}1 )</td>
</tr>
<tr>
<td>91 84 83 1 0</td>
<td>( 10^{6}610^{6}1^{2}0^{5}1010^{4}1^{4}0^{3}10^{3}1^{2}0^{2}1^{2}0 )</td>
</tr>
<tr>
<td></td>
<td>( 101010^{5}1^{8}0^{7}10^{6}1^{2}0^{5}1010^{4} )</td>
</tr>
<tr>
<td></td>
<td>( 0^{79}10^{11}1 )</td>
</tr>
<tr>
<td>92 13 12 1 0</td>
<td>( 10^{90}10 )</td>
</tr>
<tr>
<td>93 2 0</td>
<td>( 0^{73}10^{20} )</td>
</tr>
<tr>
<td>94 21 0</td>
<td>( 10^{94} )</td>
</tr>
<tr>
<td>95 11 0</td>
<td>( 10^{96} )</td>
</tr>
<tr>
<td>96 49 47 2 0</td>
<td>( 0^{47}1010^{44}10 )</td>
</tr>
<tr>
<td>97 6 0</td>
<td>( 10^{90}10^{5} )</td>
</tr>
<tr>
<td>98 11 0</td>
<td>( 0^{87}10^{10} )</td>
</tr>
<tr>
<td>99 47 45 2 0</td>
<td>( 10^{96}10 )</td>
</tr>
<tr>
<td>100 37 0</td>
<td>( 0^{63}10^{36} )</td>
</tr>
<tr>
<td>101 7 6 1 0</td>
<td>( 10^{94}10^{5} )</td>
</tr>
<tr>
<td>102 77 76 1 0</td>
<td>( 0^{25}10^{24}1^{2}0^{23}1010^{22}10 )</td>
</tr>
<tr>
<td>103 9 0</td>
<td>( 10^{102} )</td>
</tr>
<tr>
<td>104 11 10 1 0</td>
<td>( 0^{93}10^{9}1 )</td>
</tr>
<tr>
<td>105 16 0</td>
<td>( 10^{88}10^{15} )</td>
</tr>
<tr>
<td>106 15 0</td>
<td>( 0^{91}10^{14} )</td>
</tr>
<tr>
<td>107 65 63 2 0</td>
<td>( 10^{104}10 )</td>
</tr>
<tr>
<td>108 31 0</td>
<td>( 0^{77}10^{30} )</td>
</tr>
<tr>
<td>109 7 6 1 0</td>
<td>( 10^{102}10^{5} )</td>
</tr>
<tr>
<td>110 13 12 1 0</td>
<td>( 0^{97}10^{11}1 )</td>
</tr>
<tr>
<td>111 10 0</td>
<td>( 10^{100}10^{9} )</td>
</tr>
<tr>
<td>112 45 43 2 0</td>
<td>( 0^{67}1010^{42} )</td>
</tr>
<tr>
<td>113 9 0</td>
<td>( 10^{112} )</td>
</tr>
<tr>
<td>114 82 81 1 0</td>
<td>( 0^{33}10^{31}1^{2}0^{30}1010^{13}1 )</td>
</tr>
<tr>
<td>115 15 14 1 0</td>
<td>( 10^{100}10^{13} )</td>
</tr>
<tr>
<td>116 71 70 1 0</td>
<td>( 0^{45}10^{44}1^{2}0^{23}1 )</td>
</tr>
<tr>
<td>117 20 18 2 0</td>
<td>( 10^{96}1010^{15}10 )</td>
</tr>
<tr>
<td>Primitive polynomial</td>
<td>Characteristic ( m )-sequences</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>118 33 0</td>
<td>( 0^{85}10^{32} )</td>
</tr>
<tr>
<td>119 8 0</td>
<td>( 10^{11}10^{7} )</td>
</tr>
<tr>
<td>120 118 111 7 0</td>
<td>( 0^{3}10^{10}10^{1}30^{1}30^{1}20^{1}20^{1}20^{1}20^{1}20^{1} )</td>
</tr>
<tr>
<td></td>
<td>( 0^{1}30^{1}30^{1}20^{1}10^{2}10^{1}40^{1}40^{1}20^{1}20^{1}40^{1}20^{1} )</td>
</tr>
<tr>
<td></td>
<td>( 0^{2}10^{2}30^{2}10^{2}10^{2}30^{1}10^{3}10^{1}30^{2} )</td>
</tr>
<tr>
<td>121 18 0</td>
<td>( 10^{10}210^{1}7 )</td>
</tr>
<tr>
<td>122 60 59 1 0</td>
<td>( 0^{6}310^{5}71 )</td>
</tr>
<tr>
<td>123 2 0</td>
<td>( 10^{12}10 )</td>
</tr>
<tr>
<td>124 37 0</td>
<td>( 0^{8}710^{3}6 )</td>
</tr>
<tr>
<td>125 108 107 1 0</td>
<td>( 10^{16}10^{16}120^{1}510^{14}140^{1}310^{3}10^{12}120^{1} )</td>
</tr>
<tr>
<td></td>
<td>( 0^{2}1^{2}10^{1}10^{1}10^{1}0 )</td>
</tr>
<tr>
<td></td>
<td>( 0^{8}910^{3}51 )</td>
</tr>
<tr>
<td>126 37 36 1 0</td>
<td>( 10^{12}6 )</td>
</tr>
<tr>
<td>127 1 0</td>
<td>( 0^{9}910^{1}0^{2}6 )</td>
</tr>
<tr>
<td>128 29 27 2 0</td>
<td>( 10^{12}8 )</td>
</tr>
<tr>
<td>129 5 0</td>
<td>( 0^{1}2710^{2} )</td>
</tr>
<tr>
<td>130 3 0</td>
<td>( 10^{8}210^{4}7 )</td>
</tr>
<tr>
<td>131 48 47 1 0</td>
<td>( 0^{1}0^{3}10^{2}8 )</td>
</tr>
<tr>
<td>132 29 0</td>
<td>( 10^{8}010^{5}1 )</td>
</tr>
<tr>
<td>133 52 51 1 0</td>
<td>( 0^{7}710^{5}6 )</td>
</tr>
<tr>
<td>134 57 0</td>
<td>( 10^{13}4 )</td>
</tr>
<tr>
<td>135 11 0</td>
<td>( 0^{1}1^{1}0^{9}1^{2}0^{8}10^{10}7^{1}4^{0}6^{1}0^{3}10^{5}1^{2}0^{2}1^{2}0^{4} )</td>
</tr>
<tr>
<td>136 126 125 1 0</td>
<td>( 10^{1}1^{2}0^{10}3^{1} )</td>
</tr>
<tr>
<td></td>
<td>( 10^{13}6 )</td>
</tr>
<tr>
<td>137 21 0</td>
<td>( 0^{1}3110^{5}1 )</td>
</tr>
<tr>
<td>138 8 7 1 0</td>
<td>( 10^{13}010^{7} )</td>
</tr>
<tr>
<td>139 8 5 3 0</td>
<td>( 0^{1}1^{1}10^{2}8 )</td>
</tr>
<tr>
<td>140 29 0</td>
<td>( 10^{1}0^{8}10^{3}1 )</td>
</tr>
<tr>
<td>141 32 31 1 0</td>
<td>( 0^{1}2110^{2}0 )</td>
</tr>
<tr>
<td>142 21 0</td>
<td>( 10^{1}1^{2}210^{1}9 )</td>
</tr>
<tr>
<td>143 21 20 1 0</td>
<td>( 7^{5}10^{6}7 )</td>
</tr>
<tr>
<td>144 70 69 1 0</td>
<td>( 10^{9}210^{5}1 )</td>
</tr>
<tr>
<td>145 52 0</td>
<td>( 0^{8}710^{5}7 )</td>
</tr>
<tr>
<td>146 60 59 1 0</td>
<td>( 10^{1}0^{8}10^{3}7 )</td>
</tr>
<tr>
<td>147 38 37 1 0</td>
<td>( 0^{1}2110^{2}6 )</td>
</tr>
<tr>
<td>148 27 0</td>
<td>( 10^{3}810^{3}8^{1}20^{3}7^{1}0^{1}0^{2}9 )</td>
</tr>
<tr>
<td>149 110 109 1 0</td>
<td>( 0^{9}710^{5}2 )</td>
</tr>
<tr>
<td>150 53 0</td>
<td>( 10^{1}5^{0} )</td>
</tr>
<tr>
<td>151 3 0</td>
<td>( 0^{8}710^{6}3 )</td>
</tr>
<tr>
<td>152 66 65 1 0</td>
<td>( 10^{1}5^{2} )</td>
</tr>
<tr>
<td>153 1 0</td>
<td></td>
</tr>
</tbody>
</table>
### CHARACTERISTIC m-SEQUENCES

<table>
<thead>
<tr>
<th>Primitive polynomial</th>
<th>Characteristic m-sequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>154 129 127 2 0</td>
<td>$0^{25}1010^{22}10^{3}10^{20}1010101010^{18}10^{7}10^{16}$</td>
</tr>
<tr>
<td>155 32 31 1 0</td>
<td>$10^{12}210^{31}$</td>
</tr>
<tr>
<td>156 116 115 1 0</td>
<td>$0^{41}10^{39}120^{38}1010^{31}1$</td>
</tr>
<tr>
<td>157 27 26 1 0</td>
<td>$10^{13}010^{25}$</td>
</tr>
<tr>
<td>158 27 26 1 0</td>
<td>$0^{1}3110^{25}1$</td>
</tr>
<tr>
<td>159 31 0</td>
<td>$10^{15}8$</td>
</tr>
<tr>
<td>160 19 18 1 0</td>
<td>$0^{1}4110^{17}1$</td>
</tr>
<tr>
<td>161 18 0</td>
<td>$10^{14}210^{17}$</td>
</tr>
<tr>
<td>162 88 87 1 0</td>
<td>$0^{7}510^{73}120^{10}1$</td>
</tr>
<tr>
<td>163 60 59 1 0</td>
<td>$10^{16}2$</td>
</tr>
<tr>
<td>164 14 13 1 0</td>
<td>$0^{1}5110^{11}1$</td>
</tr>
<tr>
<td>165 31 30 1 0</td>
<td>$10^{13}410^{29}$</td>
</tr>
<tr>
<td>166 39 38 1 0</td>
<td>$0^{1}2710^{37}1$</td>
</tr>
<tr>
<td>167 6 0</td>
<td>$10^{16}010^{5}$</td>
</tr>
<tr>
<td>168 17 15 2 0</td>
<td>$0^{1}511010^{14}$</td>
</tr>
</tbody>
</table>

Department of Mathematics  
University of North Carolina  
Greensboro, North Carolina 27412

MR 48 #6064.