Note on decoding negacyclic Codes

K. Huber

We give a classical derivation of Roth's decoding algorithm for Berlekamp's negacyclic codes. Roth's algorithm has been presented using alternant codes. His algorithm considerably simplifies decoding. The derivation given here extends Berlekamp's original approach and should be of interest for designers not familiar with alternant codes.

Introduction: In [1], [2] Berlekamp introduced negacyclic codes for the Lee metric together with a decoding algorithm. To make this contribution self-contained his decoding algorithm is sketched in appendix A. In [3], pp. 314-317, Roth presented a simplification for the decoding of Berlekamp's negacyclic codes as special case of an algorithm for decoding alternant codes for the Lee metric. In this contribution we show how Roth's algorithm follows from the classical approach of Berlekamp without using alternant codes. This should be of interest for implementers of codes for the Lee metric.

Decoding negacyclic codes: In the following the tilde is used for the odd part of a polynomial and the hat for the even part. We start from equation (A.1) given in appendix A.

$$\tilde{S}(z)\cdot\left(\tilde{\sigma}(z)^2-\hat{\sigma}(z)^2\right)+z\cdot\left(\tilde{\sigma}(z)\hat{\sigma}'(z)-\hat{\sigma}(z)\tilde{\sigma}'(z)\right)=0 \qquad (1)$$

Use of even and odd parts of $\sigma(z)$

$$\begin{aligned}\sigma(z) &= \hat{\sigma}(z)+\tilde{\sigma}(z)\\ \sigma(-z) &= \hat{\sigma}(z)-\tilde{\sigma}(z)\end{aligned}$$

immediately gives

$$\begin{aligned}\hat{\sigma}(z) &= \frac{\sigma(z)+\sigma(-z)}{2}\\ \tilde{\sigma}(z) &= \frac{\sigma(z)-\sigma(-z)}{2}\end{aligned}$$

and when plugged into equation (1) leads to $-\tilde{S}(z)\sigma(z)\sigma(-z)+\frac{z}{4}\left((\sigma(z)-\sigma(-z))(\sigma'(z)-\sigma'(-z))-(\sigma(z)+\sigma(-z))(\sigma'(z)+\sigma'(-z))\right)=0$ which finally gives

$$-2\tilde{S}(z)\cdot\frac{\sigma(z)}{\sigma(-z)}=z\cdot\frac{\sigma(z)\sigma'(-z)+\sigma(-z)\sigma'(z)}{\sigma(-z)^2}$$

We now use the generating function

$$V(z)=\frac{\sigma(z)}{\sigma(-z)} \qquad (2)$$

$$\Rightarrow \quad V'(z)=\frac{\sigma'(z)\sigma(-z)+\sigma(z)\sigma'(-z)}{\sigma(-z)^2} \qquad (3)$$

thus

$$2\tilde{S}(z)\cdot V(z)+z\cdot V'(z)=0\,. \qquad (4)$$

The values V_i of $V(z)=1+V_1z+V_2z^2+V_3z^3+\ldots$ for $i=1,2,\ldots 2t$ are computed recursively from equation (4). For convenience the first few coefficients are given ($V_0=1$):

$$\begin{aligned}V_1 &= -2S_1V_0 && \Rightarrow V_1=-2S_1\\ V_2 &= -S_1V_1 && \Rightarrow V_2=2S_1^2\\ V_3 &= \frac{-2S_1V_2-2S_3}{3} && \Rightarrow V_3=\frac{-4S_1^3-2S_3}{3}\\ V_4 &= \frac{-2S_1V_3-2S_3V_1}{4} && \Rightarrow V_4=\frac{2S_1^4+4S_1S_3}{3}\\ &\vdots\end{aligned}$$

In general

$$V_i=\frac{-2}{i}\sum_{\substack{j+k=i\\ j\ \mathrm{odd}}}S_jV_k$$

where $i<p$. Knowing $V(z) \bmod z^{2t+1}$ we get the key-equation

$$\sigma(z)\equiv\sigma(-z)\cdot V(z) \bmod z^{2t+1}\,. \qquad (5)$$

which follows from (2). The key-equation can be solved using standard techniques, e.g. the Euclidean algorithm. Starting with the polynomials $r_{-1}(z)=z^{2t+1}$ and $r_0(z)=V(z) \bmod z^{2t+1}$ we iterate $r_k(z)=r_{k-2}(z) \bmod r_{k-1}(z)$ until the degree of the remainder polynomial $r_k(z)$ is within the bounds $1\le\deg\{r_k(z)\}\le t$. If an error of Lee-weight $1\le \mathrm{wt}\{e(x)\}\le t$ occurred, $\sigma(z)$ equals $r_k(z)$ up to a constant factor.

Example: Let us consider a $[5,3,5]$ negacyclic code over the field $GF(11)$ having generator polynomial $g(x)=(x-2)(x-2^3)$. Here $\alpha=2$ is a primitive element of $GF(11)$. To decode $r(x)=10x^4+6x^2+10x$ to the next codeword we find $S_1=r(\alpha)=6$ and $S_3=r(\alpha^3)=9$ thus $\tilde{S}(z)\equiv 6z+9z^3 \bmod z^5$. From the equations above we get $V(z)=1+V_1z+V_2z^2+V_3z^3+V_4z^4+\ldots\equiv 1+10z+6z^2+3z^3+z^4 \bmod z^5$. Execution of the Euclidean algorithm then leads to

$$z^5=(z+8)(z^4+3z^3+6z^2+10z+1)+3z^3+8z^2+7z+3$$

$$(z^4+3z^3+6z^2+10z+1)=(4z+5)(3z^3+8z^2+7z+3)+4z^2+7z+8$$

giving the error locator polynomial $\sigma(z)=(4z^2+7z+8)/8$ which has the two roots 5 and 7. Now $5\equiv 2^{-6} \bmod 11$. Hence we have an error value -1 at position $6-5=1$. From the second root $7\equiv 2^{-3} \bmod 11$ we get the error value 1 at position 3 which leads to the error polynomial $e(x)=x^3-x$.

Conclusion: Roth's simplified decoding algorithm for negacyclic codes has been derived by extending Berlekamp's classic approach.

Appendix A: Negacyclic codes: Negacyclic codes for the Lee-metric were proposed by Berlekamp in [1] and [2]. A $[n,k,d_{\mathrm{Lee}}]$ negacyclic code over the field $GF(p)$ has generator polynomial $g(x)=(x-\alpha)(x-\alpha^3)(x-\alpha^5)\ldots(x-\alpha^{2t-1})$ and minimum Lee distance $d_{\mathrm{Lee}}=2t+1$, where $2t-1<p$. The element α is an element of order $2n$ in $GF(p^m)$. Codewords $c(x)$ are multiples of $g(x)$ which divides x^n+1. After transmission the receiver gets $r(x)=c(x)+e(x)$, where $e(x)$ is an error polynomial. From the usual syndrome polynomial $S(z)=S_1z+S_2z^2+S_3z^3\ldots$ where $S_j=r(x)|_{\alpha^j}$, we only know the odd indexed syndromes and the resulting known polynomial is $\tilde{S}(z) \bmod z^{2t+1}=S_1z+S_3z^3\ldots+S_{2t-1}z^{2t-1}$. The characteristic property of Berlekamp's decoding algorithm is that only the error locator polynomial $\sigma(z)=\prod(1-\alpha^jz)$ is used to determine both, error locations and error values. An error value 1 at position l appears as root α^{-l} of $\sigma(z)$ and an error value -1 at position l as root $\alpha^{-(n+l)}=-\alpha^{-l}$, where $0\le l\le n-1$. Error values $\neq\pm1$ are characterised by multiple roots of $\sigma(z)$. Separating the odd and even parts of the Newton identities equation $S(z)\sigma(z)+z\sigma'(z)=0$ we get the two equations

$$\hat{S}\hat{\sigma}+\tilde{S}\tilde{\sigma}+z\tilde{\sigma}'=0 \quad\text{and}\quad \hat{S}\tilde{\sigma}+\tilde{S}\hat{\sigma}+z\hat{\sigma}'=0$$

Multiplying the first with $\tilde{\sigma}$ and the second with $\hat{\sigma}$ and subtracting yields

$$\tilde{S}(z)\cdot\left(\tilde{\sigma}(z)^2-\hat{\sigma}(z)^2\right)+z\cdot\left(\tilde{\sigma}(z)\hat{\sigma}'(z)-\hat{\sigma}(z)\tilde{\sigma}'(z)\right)=0\,. \qquad (A.1)$$

Berlekamp then used the generatorfunction $U(z)=\frac{\tilde{\sigma}(z)}{\hat{\sigma}(z)}$ and obtained $\tilde{S}(z)(U^2(z)-1)=zU'(z)$ which can be solved for the coefficients of $U(z) \bmod z^{2t}$. Then using $T(z^2)=\frac{1}{1+zU(z)}$ the error locator polynomial was found by solving $\omega(z)\equiv\phi(z)(1+T(z)) \bmod z^{t+1}$ for ϕ and ω. Eventually one gets the even and odd parts of σ from $\hat{\sigma}(z)=\omega(z^2)$ and $\phi(z^2)=\sigma\hat{(z)}+z\tilde{\sigma}(z)$.

K. Huber (*Huber Consult, Berlin, Germany*)

E-mail: coding@klaus-huber.net

References

1 E.R.Berlekamp, "Algebraic Coding Theory", Aegean Park Press revised edition 1984, (first edition 1968).

2 E.R.Berlekamp, "Negacyclic Codes for the Lee Metric", chap. 17 in Bose, Dowling (eds), "Proceedings of the Conference on Combinatorial Mathematics and Its Applications (April 10-14,1967)", The University of Carolina Press, Chapel Hill, published 1969.

3 R.N.Roth, "Introduction to Coding Theory", Cambridge University Press, 2006.