ードソロモン符号を(*N*，*K*)と表します．二元BCH符号では，この表記だけではいくつのエラー訂正が可能かわかりませんでしたが，リードソロモン符号では，これだけで一義的に決まります．

つまり，パリティ部分は$N-K$シンボルなので，

$$2t=N-K,\quad t=\frac{N-K}{2} \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (5\text{-}149)$$

となります．また，リードソロモン符号もBCH符号の一種で巡回符号なので，$N=2^M-1$となります．すなわち，ガロア拡大体$GF(2^M)$のMと，(*N*，*K*)が与えられれば，リードソロモン符号は一義的に決まることになります．そのため，符号語を定義するためにわざわざ生成多項式を示す必要はありません．

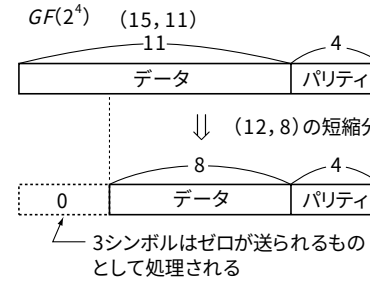

図5-33　リードソロモン符号の距離形

これまでの巡回符号のように，実際の応用で符号長が$N=2^M-1$に縛られると，とても使いにくくなります．そこで，その短縮形もよく使われます．たとえば，$GF(2^4)$の符号で，符号シンボル長が12で，データ・シンボル長が8の(12，8)のリードソロモン符号が考えられます．

図5-33のように，(15，11)のリードソロモン符号の先頭の3シンボルは，暗黙的にゼロが送られるものとして短縮するものです．そこで，短縮形の表現(*N*，*K*)で注目すべきなのは，$N-K$の値のみです．$N-K$が決まれば，何個までのエラー・シンボルが訂正可能かがわかります．すなわち，生成多項式が一意に決まります．

5.13.2　リードソロモン符号化器

リードソロモン符号もBCH符号の一種なので，二元BCH符号と作り方は同じです．符号語が生成多項式で割り切れるようにします．つまり，符号語を$T(X)$，生成多項式を$G(X)$とすると，

$$T(X)=Y(X)\cdot G(X)=Y(X)\cdot(X+\boldsymbol{\alpha})(X+\boldsymbol{\alpha}^2)\cdots\cdots(X+\boldsymbol{\alpha}^{2t}) \qquad \cdots\cdots\cdots\cdots\cdots\cdots (5\text{-}150)$$

と表せます．明らかに，$T(X)$に生成多項式の根を代入するとゼロになります．そこで，Kシンボルの送るべきデータの多項式を，

$$f(X)=G_{k-1}\cdot X^{k-1}+G_{k-2}\cdot X^{k-2}+\cdots\cdots+G_1\cdot X+G_0 \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (5\text{-}151)$$

とします．もちろん，G_jは$GF(2^M)$の元です．言い換えれば，M次のベクトルです．誤り訂正可能な最大のシンボルの個数をtとします．組織化符号とするために，上の式にX^{2t}を掛けます．符号長はNとします．

$$F(X)=X^{2t}\cdot f(X)=G_{k-1}\cdot X^{N-1}+G_{k-2}\cdot X^{N-2}+\cdots\cdots+G_1\cdot X^{2t+1}+G_0\cdot X^{2t} \qquad \cdots\cdots\cdots\cdots (5\text{-}152)$$

パリティ多項式を，

$$P(X)=L_{q-1}\cdot X^{q-1}+L_{q-2}\cdot X^{q-2}+\cdots\cdots+L_1\cdot X+L_0 \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (5\text{-}153)$$

ただし，$q=2t=N-K$

そこで，リードソロモン符号は，

$$T(X)=F(X)+P(X) \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (5\text{-}154)$$

となります．