Coding theory & Noncommutative rings.

Warsaw, 02-03 2012

Plan :

A) Coding theory - introduction

1) Definitions, sphere packings & other bounds.
2) Linear codes.
3) Polynomial & cyclic codes.
4) MacWilliams identity & theorem.

B) One extension and pseudo linear maps.

1) Definition of PLT.
2) Polynomial maps & PLT.
3) More results on polynomial maps.

C) Skew codes

1) Utility of codes based on skew polynomials.
2) $\mathbb{F}_q[x;\theta]$ and factorizations.
3) Codes based on $\mathbb{F}_q[x;\theta]$.
4) (σ,δ) - codes.

D) Codes over Frobenius rings

1) Frobenius rings & algebras.
2) Codes over commutative Frobenius rings.
3) MacWilliams identity & extension theorem.
4) Perspectives.

A) Coding theory - Introduction

1) Definitions

$$\boxed{m} \xrightarrow[1-1]{e} \boxed{m_e} \overset{t}{\underset{\text{noise}}{\rightsquigarrow}} \boxed{m_r}$$

$$\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

$n \geq k$ $\quad k/n$ rate $\quad k$ dimension $\quad n$ = length

EX : 1) Parity check $n = k+1$ $\quad \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^{k+1}$

add one bit to the message so that the sum of all bits is 0 (in $\mathbb{F}_2$)

2) Repeating the words : $n = 2k$

Morality when you increase n you can detect more errors but this ..... costs !

(Some surprise : Shannon (1948) ; information theory)

Déf. : a) $x, y \in \mathbb{F}_q^n$ $\quad d(x,y) = \#\{1 \leq i \leq n \mid x_i \neq y_i\}$

b) $C \subset \mathbb{F}_q^n$ $\quad C$ a code $\quad d(C) = \min\{d(x,y) \mid x, y \in C\}$

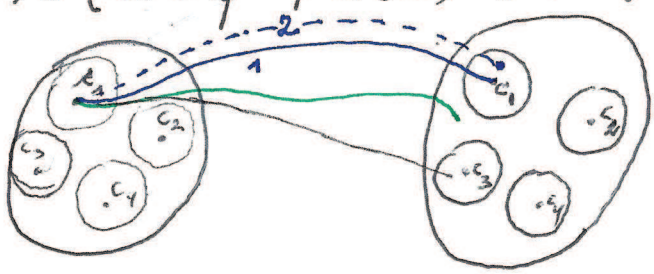
$t := \left\lfloor \frac{d-1}{2} \right\rfloor$

Remark $\quad c, c' \in C \quad B(c,t) \cap B(c',t) = \phi$

where $B(c,t) = \{x \in \mathbb{F}_q^n \mid d(x,c) \leq t\}$

EX $C = \{c_1, c_2, c_3, c_4\}$

Decoding 4 possibilities



③ <u>Theorem</u> C a code with minimal distance d. Put $t := \lfloor \frac{d-1}{2} \rfloor$. Then:

a) C can detect up to $d-1$ errors.

b) C can correct up to t errors.

<u>Problem</u> of coding theory: C a (n, M, d)-code where $|C| = M$.

1. n must be small (costs and speed)
2. $M = |C|$ must be big (big variety of messages)
3. d must be big (to detect & correct lots of errors)

<u>Bounds</u> $C \subset \mathbb{F}_q^n$ $M = |C|$

a) $M\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1) + \cdots + \binom{n}{t}(q-1)^t\right) \leq q^n$ (Hamming bound)

b) $A_q(n,d)$ maximal number of code words for a code $C \subset \mathbb{F}_q^n$ such that $d = d(C)$ then $A_q(n,d) \leq q^{n-d+1}$

2) <u>Linear codes</u>.

Déf: A code $C \subset \mathbb{F}_q^n$ is linear if C is a vector space

$\dim C =: k$ $M = |C| = q^k$ $x \in C$ $w(x) := |\{ i \mid x_i \neq 0 \}|$

<u>Property</u>: $C \subset \mathbb{F}_q^n$ $d(C) = \min \{ w(x) \mid x \in C \}$

Definitions. C a linear (n,k)-code

a) A <u>generic matrix</u> G is a $k \times n$ matrix over $\mathbb{F}_q$ such that the rows form a basis of C.

b) <u>Dual</u> of C is $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \ \forall y \in C\}$ where, for $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$, $x \cdot y = \sum_1^n x_i y_i$

c) <u>A control matrix</u> H for C is a generic matrix for $C^\perp$. Since $\dim C + \dim C^\perp = n$

$H \in M_{(n-k) \times n}(\mathbb{F}_q)$

$$H G^t = 0 \qquad G H^t = 0$$

$$C = \{x \in \mathbb{F}_q^n \mid Hx = 0\}$$

$$C^{\perp\perp} = C$$

3) Cyclic codes

Definition: A linear code $C \subset \mathbb{F}_q^n$ is cyclic if

$$(a_0, \dots, a_{n-1}) \in C \Rightarrow (a_{n-1}, a_0, \dots, a_{n-2}) \in C$$

We attached to $(a_0, \dots, a_{n-1}) \in C$ the polynomial

$$\sum_0^{n-1} a_i x^i \in \frac{\mathbb{F}_q[X]}{(X^n - 1)} \qquad (x = X + (X^n - 1))$$

(5) Hence $(a_0, \dots, a_{n-1}) \in C \longleftrightarrow g(x) = \sum a_i x^i \in \mathbb{F}_q[x]/x^n - 1$

$$(a_{n-1}, \dots, a_{n-2}) \in C \longleftrightarrow g(x)\, x$$

In this way cyclicity corresponds to stability by left multiplication by x, ...

$\mathbb{F}_q^n \supset$ cyclic codes $\longleftrightarrow$ ideals of $\mathbb{F}_q[X]/(X^n - 1)$

$\mathbb{F}_q^n \supset$ cyclic codes $\longleftrightarrow$ factors of $X^n - 1$

$\mathbb{F}_q^n \supset C \longleftrightarrow g(x)\, \mathbb{F}_q[x] \qquad g(X) \mid X^n - 1$

$\dim_{\mathbb{F}_q} C = k \longleftrightarrow \deg g(X) = n - k$

<u>Theorem</u> $C \subset \mathbb{F}_q^n$ a cyclic code with associated polynomial $g(x) = g_0 + g_1 x + \dots + g_{n-k} x^{n-k}$

the generic matrix is given by

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & & g_{n-k} & 0 \cdots & 0 \\ 0 & 0 & g_0 & \cdots & & & \\ & & & & & & \\ 0 & \cdots & & & & & \end{pmatrix} \in M_{k \times n}(\mathbb{F}_q)$$

the control matrix (aka as parity check matrix)

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \cdots & 0 \\ & & & & & & & \\ 0 & & & h_k & \cdots & & & h_0 \end{pmatrix} \in M_{n-k \times n}(\mathbb{F}_q)$$

where $g(X)\, h(X) = X^n - 1 \qquad h(X) = h_0 + h_1 X + \dots + h_k X^k$

check polynomial.

Example ① Golay code $X^{23}-1 = (X-1)\, g(X)\, g_1(X)$

where $g(X) = X^{11} + X^{9} + X^{7} + X^{6} + X^{5} + X + 1$

$g_1(X) = X^{11} + X^{10} + X^{6} + X^{5} + X^{4} + X^{2} + 1$

These two polynomials are reciprocal of each other ($g_1(x) = X^{11} g(x^{-1})$ & $g(x) = X^{11} g_1(x^{-1})$) and hence generate equivalent codes ... these codes are cyclic (23, 12)-codes with generator $g(x) \in \mathbb{F}[x]_{23}$. The code word corresponding to $g(x)$ is of weigth 7 and in fact it gives the minimal weight i.e. $d(G_{23}) = 7$. It can correct up to 3 errors.

G_{23} is a perfect code (The sphere packing bound is obtained)

Corollary If $C \subset \mathbb{F}_q^{\,n}$ is a cyclic code then $C^{\perp}$ is cyclic as well. (with generating polynomial equal to the reciprocal of the annihilator of the generator of C)

4) MacWilliams identity and theorem

<u>Definition</u> $C \subset \mathbb{F}_q^n$ a linear code. The weight enumerator polynomial is $W_C = \sum_{i=0}^{n} \omega_i x^{n-i} y^i$ where $\omega_i = |\{\text{words in } C \text{ of weight } i\}|$

<u>EX</u>: $C = \{000, 111\} \subset \mathbb{F}_2^3$ $\quad W_C(x,y) = x^3 + y^3$

(!) $C^\perp = \{000, 011, 101, 110\}$ $\quad W_{C^\perp}(x,y) = y^3 + 3xy^2$

<u>Théorème</u> (MacWilliams 1962) $C \subset \mathbb{F}_q^n$ linear

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x + (q-1)y, x-y)$$

<u>EX 1</u> $C = \{000, 111\}$ $\quad C^\perp = \{000, 110, 101, 011\}$

$W_C(x,y) = x^3 + y^3$ $\quad W_{C^\perp}(x,y) = x^3 + 3xy^2$

<u>EX2</u> C the linear code of length 8 with generic matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad C = C^\perp$$

$$W_C = x^8 + 14x^4y^4 + y^8 = W_{C^\perp}$$

<u>Definitions</u> (a) $T: \mathbb{F}_q^n \to \mathbb{F}_q^n$ is called a monomial transformation if there exists $\sigma \in S_n$ and $u_1, \dots, u_n \in \mathbb{F}_q^*$ such that $T(x_1, \dots, x_n) = (x_{\sigma(1)} u_1, \dots, x_{\sigma(n)} u_n)$

(b) $C_1 \subset C_2 \subset \mathbb{F}_q^n$ linear codes are monomially equivalent if there exists a mon. tsf T s.t $T(C_1) = C_2$

e) A linear isomorphism $f : C_1 \longrightarrow C_2$ between linear codes in $\mathbb{F}_q^n$ is an isometry if it preserves Hamming weight : $wt(f(x)) = wt(x)$

<u>MacWilliams Extension Theorem</u> : C_1, C_2 two linear codes in $\mathbb{F}_q^n$; $f : C_1 \to C_2$ a linear isomorphism. Then:

f is an isometry iff f extends to a monomial transf of $\mathbb{F}_q^n$

B) $\boxed{\text{Ore extensions and pseudo linear maps.}}$

1) Let A be a ring $\sigma \in End(A)$ δ a σ-derivation of A and $R = A[t; \sigma, \delta]$. If ${}_RV$ is a left R-module then ${}_AV$ is a left A-module and

$$ta.v = \sigma(a)t.v + \delta(a)v = t.(av)$$

This motivates : $T : {}_AV \to {}_AV$ is a <u>(σ, δ) P.L.T.</u> if T is A-linear and $T(av) = \sigma(a)T(v) + \delta(a)v$

<u>Theorem</u> There is a correspondence between

left R-modules $\longleftrightarrow$ (σ, δ)-PLT on left A-modules

<u>Definition</u> $f(t) \in R = A[t; \sigma, \delta]$ $a \in A$ $f(a) \in A$ defined by $f(t) - f(a) \in R(t-a)$

<u>Propriétés</u> $f(t), g(t) \in R$ $a \in A$ T_a σ, δ PLT

a) $f(T)g(T) = (fg)(T)$, where $(\sum a_i t^i)(T) = \sum a_i T^i$.

b) $f(a) = f(T_a)(1)$, where $T_a(x) = \sigma(x)a + \delta(x)$.

c) $(fg)(a) = f(T_a)(g(a))$.

d) If $g(a) \in U(A)$ $(fg)(a) = f(a^{g(a)})g(a)$
where $a^e = \sigma(e)ae^{-1} + \delta(e)e^{-1}$ $e \in U(A)$.

<u>Applications to Ore extensions over finite fields.</u>

We can restrict to Ore extensions $\mathbb{F}_q[x;\sigma]$ where $\sigma \in Aut(\mathbb{F}_q)$.

Let $\Theta : \mathbb{F}_q \to \mathbb{F}_q$ be the Frobenius automorphism $\Theta(a) = a^p$, $a \in \mathbb{F}_q$.

Let x be a commuting indeterminate over $\mathbb{F}_q$ we can extend Θ to $\mathbb{F}_q[x]$ & consider $\mathbb{F}_q[x][t;\Theta]$ $(\Theta(x) = x^p)$. We note

a) For $i \geq 1$ $[i] = \frac{p^i - 1}{p-1} = p^{i-1} + p^{i-2} + \cdots + p + 1$
and put $[0] = 0$.

b) $\mathbb{F}_q[x^{[\,]}] = \{\sum_{i \geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x]\}$

We can consider evaluation at x and get the evaluation map : $\mathbb{F}_x[x][t;\Theta] \longrightarrow \mathbb{F}_q[x]$ and hence

$$\mathbb{F}_q[t;\theta] \hookrightarrow \mathbb{F}_q[x][t;\theta] \longrightarrow \mathbb{F}_q[x]$$
$$p(t) \longmapsto p(x) = p(T_x)(1)$$

This is used in connection with T_x to get the factorizations results in the second part of the following

<u>Theorem</u> (L.)

A) The polynomial $G(t) := t^{(p-1)n+1} - t$ is the least left common multiple of $t-a$, $a \in \mathbb{F}_{q=p^n}$ in $\mathbb{F}_q[t;\theta]$. We have $RG = GR$.

B) For $a \in \mathbb{F}_q$, $f(t) = \sum a_i t^i \in R = \mathbb{F}_q[t;\theta]$

1) $f(b) = \sum a_i b^{[i]}$

2) $f(t)(x) = \sum a_i x^{[i]} =: f^{[\,]}(x)$

3) $\{f^{[\,]} \mid f \in R = \mathbb{F}_q[t;\theta]\} = \mathbb{F}_q[x^{[\,]}]$

4) $h(t) \in R = \mathbb{F}_q[t;\theta]$, $f(t) \in Rh(t)$ if and only if $f^{[\,]}(x) \in \mathbb{F}_q[x]\, h^{[\,]}(x)$

5) factorization of $f(t) \in \mathbb{F}_q[t;\theta]$ can be obtained from factorization in $\mathbb{F}_q[x]$

6) $f(t)$ is irreducible in R iff $f^{[\,]}$ is $[\,]$-irreducible

There are many more factorizations in $\mathbb{F}_q[t;\theta]$ then in $\mathbb{F}_q[x]$. This is one of the reasons that these rings were used in coding theory (Boucher, Solé, Ulmer ....

We will show how the PLT's seem to be useful in the more general frame of $R = A[t;\sigma,\delta]$

E) Codes with skew polynomials.

Ulmer, Boucher, Solé, ... used $\mathbb{F}_q[X;\theta]$ to construct codes. The advantage is that there are a lot of dist. factorizations of a given polynomial

<u>EX</u> $X^4+X^2+1 = (X^2+X+1)^2$ in $\mathbb{F}_4[X;\theta]$

$$= (X^2+\alpha^2)(X^2+\alpha) \qquad \alpha^2+\alpha+1=0$$
$$= (X^2+\alpha)(X^2+\alpha^2)$$
$$= (X^2+\alpha^2X+1)(X^2+\alpha^2X+1)$$
$$= (X^2+\alpha X+1)^2$$

Hence they discovered new (cyclic) codes with larger distances then the known codes of the same length.

Using P.L.T it is possible to go further:

<u>Definition</u> $f \in R = A[t;\sigma,\delta]$ monic of degree n.

A (σ,δ)-code $C \subset A^n$ is the set of n-tuples corresponding to the left R-module Rg/Rf where $g_r \mid f$. Put $\deg g = r$ We get back "cyclicity" & "Generic matrix":

<u>Theorem (Boulagouaz, L)</u>

a) $\underline{v} := (a_0, \dots, a_{n-1}) \in C \Rightarrow T_f(v) \in C$

b) The n-tuples defined by $(T_f)^k(g_0, \dots, g_r)$ for $0 \leq k \leq n-r-1$ generate the code C

This gives back the θ-codes defined over $\mathbb{F}_q$

- $(a_0, \dots, a_{n-1}) \in C_\theta \to (\theta(a_0), \dots, \theta(a_{n-1})) \in C$

- $$G = \begin{pmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{r-1}) & \theta(g_r) & 0 & \cdots & 0 \\ 0 & 0 & \theta^2(g_0) & \cdots & \theta^2(g_{r-1}) & \theta^2(g_r) & 0 & \cdots \\ & & & & & & & \\ 0 & \cdots & & 0 & \theta^{n-r-1}(g_0) & \cdots & & \end{pmatrix}$$

If we write $f = gh$ in R, the code C corresponds to $\mathrm{lann}_{R/Rf}\, h$ this can be used to get a control map

i.e. $(c_0, \dots, c_{n-1}) \in C \longleftrightarrow \sum c_i T_f^i(\underline{h}) = \underline{0}$

Another way of building codes with $R = A[t; \sigma, \delta]$ is to consider $L \subset R$ of polynomials $t - a_1, \dots, t - a_n$

the control map is easier to get since we just need to verify that $a_1, \dots, a_n$ are roots...

D) Codes over Frobenius rings.

1) Frobenius rings & algebras.

Theorem - definition

A ring R is a quasi-Frobenius ring if it satisfies the following equivalent conditions:

(1) R is right noetherian and right self injective.

(2) R is left noetherian and right self-injective.

(3) R is right noetherian and satisfies the following double annihilator conditions: (3a) $\mathrm{ann}_r(\mathrm{ann}_l I) = I$ for any right ideal $I \subseteq R$

(3b) $\mathrm{ann}_l(\mathrm{ann}_r(J)) = J$ for any left ideal $J \subseteq R$

(4) R is (a-sided) artinian and satisfies (3a) and (3b).

(5) A right R-module is projective iff it is injective.

Let $J := \mathrm{rad}(R)$ be the Jacobson radical of a ring R

Then the following are equivalent

(i) R is Q.F. and $\mathrm{soc}(R_R) \cong (R/J)_R$

(ii) R is Q.F. and $\mathrm{soc}({}_RR) \cong {}_R(R/J)$

(iii) $\mathrm{soc}(R_R) \cong (R/J)_R$ and $\mathrm{soc}({}_RR) \cong {}_R(R/J)$

Examples

1) Any semisimple ring is a Frobenius ring.

2) $\mathbb{Z}/n\mathbb{Z}$

3) $k[t]/(f)$ $(f \neq 0)$

4) If R is commutative R is Frobenius iff R is Q.F. iff $R \cong R_1 \times \cdots \times R_s$ where each R_i is a local artinian ring with a simple soc.

5) For any finite dimensional k-algebra R, the following are equivalent

(i) R is a Frobenius ring

(ii) There exists a non singular bilinear pairing $B: R \times R \to k$ s.t. $B(xy, z) = B(x, yz)$ for $x, y, z \in R$

(iii) There exists a linear subspace of codimension 1 $H \subseteq_k R$ which contains no nonzero right ideal

(iv) $\mathrm{Hom}_k(R, k) \cong R$ as right R-modules.

(v) $\mathrm{Hom}_k(R, k) \cong R$ as left R-modules.

6) G a finite group k field kG is a Frobenius ring

7) H a finite-dimensional Hopf algebra then H is F.R.

In coding theory finite rings are used

Recall G a finite abelian group

A character $\chi : G \to \mathbb{C}$ is a function such that

$\chi(g+h) = \chi(g)\chi(h)$

R a finite ring, χ a character of $R,+$; $a \in R$

${}^{(a)}\chi : R,+ \longrightarrow \mathbb{C}$ defined by ${}^{(a)}\chi(x) = \chi(ax)$ $\quad x \in R$

$\chi^{(a)} : R,+ \longrightarrow \mathbb{C}$ defined by $\chi^{(a)}(x) = \chi(xa)$ $\quad x \in R$

The set $\hat{R}$ of characters of $R,+$ becomes an (R,R)-bimodule

Via : $a \in R$ $\quad \chi \in \hat{R}$ $\quad a.\chi = {}^{(a)}\chi$ and $\chi.a = \chi^{(a)}$

<u>Theorem (Hirano)</u> R a finite ring. Then the following are equivalent : (1) ${}_R R \cong {}_R\hat{R}$ as left R-modules

(2) $R_R \cong \hat{R}_R$ as right R-modules.

(3) R is a Frobenius ring.

(Honold) $\left\{ \begin{array}{l} (4)\ {}_R(R/J) \cong soc({}_R R) \text{ as left } R\text{-modules} \\ (5)\ (R/J)_R \cong soc(R_R) \text{ as right } R\text{-modules} \end{array} \right.$

Examples ⓐ Finite fields $\mathbb{F}_q$ $\quad \chi(x) = e^{2i\pi Tr(x)/p}$

ⓑ $\mathbb{Z}/m\mathbb{Z}$ $\quad \chi(x) = e^{2i\pi x/m}$

ⓒ Galois rings (Galois extensions of $\mathbb{Z}/p^m\mathbb{Z}$)

ⓓ Finite chain rings

ⓔ Products of Frobenius rings

ⓕ Matrix rings over F. R.

Theorem over finite

1

Frobenius ring, o

s. If $f: E_1 \to E_2$

ing weight then

f is an

2) MacWilliams identity and MacWilliams extension theorem

<u>Theorem</u> (Wood)

R a finite Frobenius ring. $C \subset R^n$ a left linear code, then the MacWilliams identity holds $W_C(X,Y) = \frac{1}{|r(C)|} W_{r(C)}(X+(|R|-1)Y, X-Y)$

where $r(C) = \{ y=(y_1,\dots,y_n) \in R^n \mid \sum_{i=1}^{n} c_i y_i = 0 \text{ for } (c_1,\dots,c_n) \in C \}$

MacWilliams extension Theorem over finite rings

<u>Theorem Wood, 1999</u>

Let R be a finite Frobenius ring, and suppose $C_1, C_2 \subset R^n$ are left linear codes. If $f: C_1 \to C_2$ is an R-linear isomorphism that preserves Hamming weight then f extends to a monomial transformation of R^n i.e. there exist $\sigma \in S_n$ and $u_1, \dots, u_n \in U(R)$ such that $f(x_1,\dots,x_n)$

$= (x_{\sigma(1)} u_1, x_{\sigma(2)} u_2, \dots, x_{\sigma(n)} u_n)$ for $x_1, \dots, x_n \in R$.

In fact finite Frobenius rings are characterized by the extension theorem:

<u>Theorem (Wood, 2008)</u> Suppose R is a finite ring. If the extension theorem for Hamming weight holds for linear codes over R, then R is a Frobenius ring.

Bibliography

This is a very partial (commented) bibliography
(Uwaga: Przepraszam obiecalem ze to zrobie...dobrze ze nie powiedzialem kiedy).

(1) D. Boucher, W. Geiselmann, F. Ulmer Skew-cyclic codes, Applied Algebra in Engineering, Communication and Computing, Volume 18, Number 4, p. 379-389 (2007).

(2) D. Boucher, F. Ulmer: Linear codes using skew polynomials with automorphisms and derivations, available on Hal since May 31st. Comments: D. Boucher and F. Ulmer

Comments: The codes are defined on a finite field and use inner derivations. Of course, the Ore extension is then of automorphism form but it seems that nevertheless it is interesting to consider this case since the transformation required for erasing the derivation (a change of variables=cv transformations)does not preserve Hamming distance.

(3) Dougherty, self dual codes over commutative Frobenius rings.

Comments: Steven's web page is also worth to visit:

https://sites.google.com/site/professorstevendougherty/home

(4) Honold : Characterization of finite Frobenius rings, Arch. Math. 76 (2001) 406-415.

(5) M. Ikeda A Characterization of Quasi-Frobenius Rings, Osaka Mathematical journal Vol. 4, No, 2, December, 1952.

Comments: In this paper a characterization of quasi-Frobenius rings using extensions of modules maps between ideals is given in term of extension of maps via multilplication by some elements. It seems to me that this is close enough to the MacWilliams extension theorem to be mentioned here. Actually I am a bit surprised that this paper is nearly never mentioned anywhere.

(6) Jay A. Wood Applications of finite Frobenius Rings to the foundations of codinfg theory This is one of the many papers Jay Wood has written on the subject.

Comments: It seems to me that it is better (and easier) to redirect you to his web page which contains many interesting papers and PDF of slides from talks he gave around the world.So here is the URL: http://homepages.wmich.edu/ jwood/