Finite Frobenius Rings and Their Applications

Xiang-dong Hou
Department of Mathematics
University of South Florida

May 16, 2007
Lecture 1

Quasi-Frobenius Rings and Frobenius Rings

• Quasi-Frobenius Rings

• Frobenius Rings

• The Character Module

• The Extension Property
Quasi-Frobenius Rings

Quasi-Frobenius rings. A left noetherian ring $R$ is called quasi-Frobenius (QF) if $R_R$ is an injective module. Recall that an $R$-module $R^A$ is called injective if for every injection $i : A \rightarrow B$ and $R$-map $f : A \rightarrow E$, there exists an $R$-map $g : B \rightarrow E$ such that

\[
\begin{array}{ccc}
0 & \rightarrow & A \rightarrow^i B \\
 & \downarrow f & \downarrow g \\
 & E & \end{array}
\]

commutes.
Left and right annihilators.

Let $R$ be a ring and $S \subset R$. The left and right annihilators of $S$ are respectively

$$l(S) = \{ x \in R : xs = 0 \forall s \in S \},$$
$$r(S) = \{ x \in R : sx = 0 \forall s \in S \}.$$

**Theorem 1** $R$ is QF $\iff$ $R$ is left noetherian and for every left ideal $A$ and right ideal $B$ of $R$, $l(r(A)) = A$ and $r(l(B)) = B$.

**Facts.**

(i) The definition of QF rings and the statement of Theorem 1 are left-right symmetric.

(ii) A QF ring is artinian (left and right).

**Theorem 2** A ring $R$ is QF iff projective $R$-modules are precisely injective $R$-modules.
Proposition 3 Let $R$ be a right artinian ring and $J = \text{rad } R$. Let $1_R = e_1 + \cdots + e_n$ be a decomposition of $1_R$ into orthogonal primitive idempotents.

(i) Every non nilpotent right ideal $I$ of $R$ contains an idempotent.

(ii) Every right ideal properly contained in $e_i R$ is nilpotent.

(iii) $e_i R / e_i J$ is a simple $R$-module.

(iv) Let $M$ be a simple right $R$-module. Then $M e_i \neq 0 \Leftrightarrow M \cong e_i R / e_i J$. 

Proposition 4 let $R$ be a QF ring and let $e$ be a primitive idempotent of $R$. Let $J = \text{rad } R$. Then $l(J)e$ is the unique simple submodule of $Re$ and $Re$ is the injective hull of $l(J)e$.

Proof. 1° $l(J)e$ is simple. We have

$$l(J)e = l(eJ) \cap Re = l(eJ) \cap l((1 - e)R) = l(eJ + (1 - e)R).$$

Since

$$\frac{R}{eJ + (1 - e)R} \cong \frac{eR \oplus (1 - e)R}{eJ \oplus (1 - e)R} \cong eR/eJ$$

is simple, $eJ + (1 - e)R$ is a maximal right ideal of $R$. Since $R$ is QF, $l(eJ + (1 - e)R)$ is a minimal left ideal of $R$.

2° $Re$ is the injective hull of $l(J)e$. Since $Re$ is projective and $R$ is QF, $Re$ is injective. Thus $Re$ contains an injective hull $H$ of $l(J)e$. Since $H$ is injective, $Re = H \oplus H'$ for some submodules $H' \subset Re$. Since $Re$ is indecomposable, $Re = H$. 

5
3° $l(J)e$ is the unique simple submodule of $Re$. It suffices to show that $Re$ is essential over $l(J)e$, i.e., $l(J)e$ has a nonzero intersection with any nonzero submodule of $Re$. Since $Re$ is injective, $Re$ contains a maximal essential extension $M$ of $l(J)e$ ([Lam98, Proof of Lemma 3.29]). It suffices to show $M = Re$. By Zorn’s lemma, $\exists$ submodules $A \subset Re$ maximal with respect to the property that $A \cap M = 0$. Then in $Re/A$, any nonzero submodule $B/A$ intersects $A \oplus M/A$ nontrivially. So $Re/A$ is essential over $A \oplus M/A \cong M$. By the maximality of $M$, we have $Re/A = A \oplus M/A$, i.e., $Re = A \oplus M$. Thus $M$ is injective. By 2°, $M = Re$. 
Frobenius Rings

Nakayama permutation and Frobenius rings.

Let $R$ be a QF ring and let

$$1_R = e_{11} + \cdots + e_{1m_1} + \cdots + e_{t1} + \cdots + e_{tm_t} \quad (1)$$

be a decomposition of $1_R$ into orthogonal primitive idempotents, where $e_{ij} \cong e_{kl}$ iff $i = k$. (If $e$ and $f$ are idempotents of a ring $R$, $e \cong f$ means that $eR \cong fR$, which is equivalent to $Re \cong Rf$. Cf. [Lam91, Prop. 21.20].) Put $e_i = e_{i1}$, $1 \leq i \leq t$. By Proposition 3 (iv) and Proposition 4, $\exists$ a function $\pi : \{1, \ldots, t\} \rightarrow \{1, \ldots, t\}$ such that

$$l(J)e_i \cong Re_{\pi(i)}/Je_{\pi(i)}, \quad 1 \leq n_i \leq t.$$

If $\pi(i) = \pi(k)$, then $l(J)e_i \cong l(J)e_k$, hence $Re_i = E(l(J)e_i) \cong E(l(J)e_k) = Re_k$. So $i = k$. Thus $\pi$ is a permutation of $\{1, \ldots, t\}$; it is
called the (left) Nakayama permutation of $R$. We have

$$e_iR/e_iJ \leftrightarrow (e_iR/e_iJ)^{**}$$

$$\cong (l(J)e_i)^* \text{ (note below)}$$

$$\cong (Re_{\pi(i)}/Je_{\pi(i)})^* \text{ (note below)}$$

$$\cong e_{\pi(i)}r(J).$$

So,

$$e_iR/e_iJ \cong e_{\pi(i)}r(J). \quad (2)$$

Therefore, the right Nakayama permutation of $R$ is $\pi^{-1}$. $R$ is called Frobenius if $m_i = m_{\pi(i)}$, $1 \leq i \leq t$.

**Note.** $A^* = \text{Hom}_R(A, R)$ is the dual module of $A$. If $R$ is QF and $e$ is a primitive idempotent of $R$, then

$$(Re/Je)^* \cong er(J), \quad (eR/eJ)^* \cong l(J)e.$$
Theorem 5 Let $R$ be an artinian ring and let $ar{R} = R/\text{rad } R$. Then the following statements are equivalent

(i) $R$ is Frobenius.

(ii) $R$ is QF and $\text{soc}(R_R) \cong R \bar{R}$.

(iii) $R$ is QF and $\text{soc}(R_R) \cong \bar{R}_R$.

(iv) $\text{soc}(R_R) \cong R \bar{R}$ and $\text{soc}(R_R) \cong \bar{R}_R$.

Note. If $|R| < \infty$, then (iv) $\Leftrightarrow \text{soc}(R_R) \cong R \bar{R}$ or $\text{soc}(R_R) \cong \bar{R}_R$, see [Hon01].

The proof uses the following

Proposition 6 Let $R$ be an artinian ring. Then $R$ is QF $\Leftrightarrow$ the dual of every simple left or right $R$-module is simple.
The Character Module

The character module. Let $\hat{\mathcal{A}} \equiv \text{Hom}_{\mathbb{Z}}(\mathcal{A}, \mathbb{C}^{\times})$. Then $\hat{\mathcal{A}}$ is a right $R$-module. (\forall f \in \hat{\mathcal{A}} \text{ and } r \in R, fr \in \hat{\mathcal{A}} \text{ is defined by } (fr)(x) = f(rx) \forall x \in R.)$ $\hat{\mathcal{A}}$ is called the character module of $\mathcal{A}$.

If $\phi \in \text{Hom}_{R}(\mathcal{A}, \mathcal{B})$, define

\[
\hat{\phi} : \hat{\mathcal{B}} \rightarrow \hat{\mathcal{A}} \\
\hat{f} \mapsto f \circ \phi.
\]

Then $\hat{\phi} \in \text{Hom}_{R}(\hat{\mathcal{B}}, \hat{\mathcal{A}})$. Moreover, $\hat{(} : \text{R}\text{M} \rightarrow \text{M}_{R}$ is a contravariant functor.

Similarly, if $\mathcal{A}$ is a right $R$-modules, the character module of $\mathcal{A}$ is defined to be $\hat{\mathcal{A}} = \text{Hom}_{\mathbb{Z}}(\mathbb{Z} \mathcal{A}, \mathbb{Z} \mathbb{C}^{\times})$, which is a left $R$-module. If $\phi \in \text{Hom}_{R}(\mathcal{A}, \mathcal{B})$, also define $\hat{\phi} : \hat{\mathcal{B}} \rightarrow \hat{\mathcal{A}}$ by $\phi(f) = f \circ \phi$. Then $\hat{\phi} \in \text{Hom}_{R}(\hat{\mathcal{B}}, \hat{\mathcal{A}})$ and $\hat{(} : \text{M}_{R} \rightarrow \text{R}\text{M}$ is a contravariant functor.
The character group. Let $A$ be an abelian group ($\mathbb{Z}$-module). Then $\hat{A} = \text{Hom}_\mathbb{Z}(A, \mathbb{C}^\times)$ is the character group of $A$. When $|A| < \infty$, $A \cong \hat{A}$ (non canonically).

The character module of a finite module. If $_RA$ is a finite left $R$-module, then for each $f \in \text{Hom}_\mathbb{Z}(RA, \mathbb{C}_\mathbb{Z}^\times)$, $\exists! g \in \text{Hom}_\mathbb{Z}(RA, (\mathbb{Q}/\mathbb{Z})_\mathbb{Z})$ such that
\[ f = \alpha \circ g, \]
where $\alpha : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times$, $r + \mathbb{Z} \mapsto e^{r2\pi i}$. Thus the character module of $_RA$ can also be defined as $A^b = \text{Hom}_\mathbb{Z}(RA, (\mathbb{Q}/\mathbb{Z})_\mathbb{Z})$. (If $A_R$ is a finite right $R$-module, then $A^b = \text{Hom}_\mathbb{Z}(ZA_R, \mathbb{Z}(\mathbb{Q}/\mathbb{Z})).$) Let $\mathcal{M}_R^0$ ($\mathcal{M}_R^0$) denote the category of finite left (right) $R$-modules. Then $( )^b : \mathcal{M}_R^0 \to \mathcal{M}_R^0$ and $( )^b : \mathcal{M}_R^0 \to \mathcal{M}_R^0$ are contravariant functors.
Fact. \( (\ )^{bb} : R\mathcal{M}^0 \to R\mathcal{M}^0 \) is naturally equivalent to the identity functor of \( R\mathcal{M}^0 \). The same is true for \( (\ )^{bb} : \mathcal{M}_R^0 \to \mathcal{M}_R^0 \).

Proposition 7 Let \( R \) be a finite ring, \( J = \text{rad} R \), and \( e \) a primitive idempotent of \( R \). Then

\[
(Re/Je)^{b} \cong eR/eJ. \tag{3}
\]

Generating characters. Let \( R \) be a finite ring. The character group

\[
(R, +)^{b} = \text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})
\]

is an \( (R, R) \)-bimodule since \( R \) is an \( (R, R) \)-bimodule. A character \( \chi \in (R, +)^{b} \) is called a generating character of \( R \) if \( (R, +)^{b} = R\chi \).
Proposition 8 Let $R$ be a finite ring and $\chi \in (R, +)^\flat$. The following statements are equivalent.

(i) $\chi$ is a generating character of $R$.

(ii) The map $(R, +) \to (R, +)^\flat$, $a \mapsto \chi(\cdot a) = a\chi$ is a left $R$-module isomorphism.

(iii) $\ker \chi$ does not contain any nonzero left ideal.

Proposition 9 Let $R$ be a finite ring and $\chi$ a generating character of $R$. Then there is an automorphism (the Nakayama automorphism) $\eta$ of $R$ such that

$$
\chi(yx) = \chi(x\eta(y)) \quad \forall x, y \in R.
$$

(4)
Corollary 10  The definition of generating characters and the statements in Proposition 8 are left-right symmetric.

Theorem 11 (J. Wood 99) Let $R$ be a finite ring. Then the following statements are equivalent.

(i) $R$ is Frobenius.

(ii) $R$ has a generating character $\chi$.

(iii) $(RR)^\flat \cong RR$.

(iv) $(RR)^\flat \cong R_R$. 
Proof. 1° (iii) or (iv) ⇒ (i). Obvious since \( R \) and \( R_R \) are cyclic \( R \)-modules.

2° (ii) ⇒ (iii) and (iv). Define
\[
\phi : R_R \longrightarrow (R_R)^b, \quad a \mapsto \chi(\cdot a), \quad \psi : R_R \longrightarrow (R_R)^b, \quad a \mapsto \chi(a \cdot).
\]
Then \( \phi \) and \( \psi \) are isomorphisms.

3° (ii) ⇒ \( R \) is QF. Let \( L \) be a left ideal of \( R \). Since \( \chi \) is a generating character of \( R \), the map \((R,+) \rightarrow (R, +)^b, a \mapsto \chi(\cdot a)\) is onto. Since the restriction map \((R, +)^b \rightarrow L^b\) is also onto, \( f : R \rightarrow L^b, a \mapsto \chi(\cdot a)|_L \), is an onto homomorphism of abelian groups. Since \( \ker f = r(L) \), we have \( R/r(L) \cong L^b \). In particular, \( |R/r(L)| = |L^b| = |L| \), i.e., \( |r(L)| = \frac{|R|}{|L|} \). In the same way, \( |l(J)| = \frac{|R|}{|J|} \) for every right ideal \( J \) of \( R \). Thus \( |r(l(J))| = \frac{|R|}{|l(J)|} = |J| \). Since \( J \subset r(l(J)) \), we have \( r(l(J)) = J \). In the same way, \( l(r(L)) = L \). Therefore \( R \) is QF.
4° (i) ⇔ (iii). (By symmetry, we have (i) ⇔ (iv).) By 1° and 3°, we may assume that $R$ is already QF. Let
\[ 1_R = e_{11} + \cdots + e_{1m_1} + \cdots + e_{t1} + \cdots + e_{tm_t} \]
be a decomposition of $1_R$ into orthogonal primitive idempotents, where $e_{ij} \cong e_{kl}$ iff $i = k$. Put $e_i = e_{i1}$, $1 \leq i \leq t$. Then $R_R = \bigoplus_i m_i \cdot Re_i$, so
\[ (R_R)^b \cong \bigoplus_i m_i \cdot (Re_i)^b. \]
Since $Re_i$ is indecomposable, so is $(Re_i)^b$. Since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, $(R_R)^b = \text{Hom}_\mathbb{Z}(R_R \mathbb{Z}, (\mathbb{Q}/\mathbb{Z}) \mathbb{Z})$ is an injective $R$-module. So $(Re_i)^b$ is injective. From $Re_i \twoheadrightarrow Re_i/Je_i$, we have
\[ (Re_i)^b \twoheadleftarrow (Re_i/Je_i)^b \cong e_i R/e_i J, \]
where the isomorphism is from Proposition 7. Thus $(Re_i)^b \cong$ the injective hull of $e_i R/e_i J$. By (2), $e_i R/e_i J \cong e_{\pi(i)} r(J)$, where $\pi$ is the Nakayama permutation of $R$, and by Proposition 4, $e_{\pi(i)} R$ is the injective hull of $e_{\pi(i)} r(J)$. So
\[ (Re_i)^b \cong e_{\pi(i)} R. \]
Thus
\[ (R_R)^b \cong \bigoplus_i m_i \cdot (Re_i)^b \cong \bigoplus_i m_i \cdot e_{\pi(i)} R = \bigoplus_i m_{\pi^{-1}(i)} \cdot e_i R. \]
Meanwhile, $R_R = \bigoplus_i m_i \cdot e_i R$. So
\[ (R_R)^b \cong R_R \Leftrightarrow m_{\pi^{-1}(i)} = m_i \ \forall i \Leftrightarrow R \text{ is Frobenius}. \]
The Extension Property

Codes over modules. Let $R$ be a finite ring and $\mathcal{R}A$ a finite $R$-module. For $a = (a_1, \ldots, a_n) \in A^n$, the Hamming weight of $a$ is defined to be $|a| = |\{i : 1 \leq i \leq n, \ a_i \neq 0\}|$. An $R$-submodule of $A^n$ is called a linear code of length $n$ over $A$. A monomial transformation of $A^n$ is an $R$-automorphism $A^n \rightarrow A^n$ of the form

$$f(a_1, \ldots, a_n) = (\phi_1(a_{\rho(1)}), \ldots, \phi_n(a_{\rho(n)})),$$

$$(a_1, \ldots, a_n) \in A^n,$$

where $\rho$ is a permutation of $\{1, \ldots, n\}$ and $\phi_1, \ldots, \phi_n \in \text{Aut}_R(A)$. Monomial transformations of $A^n$ are precisely the automorphism which preserves the Hamming weight; they are the isometries of $A^n$ with respect to the Hamming distance.
More generally, let $C_1, C_2 \subset A^n$ be two linear codes. An $R$-isomorphism $g : C_1 \rightarrow C_2$ which preserves the Hamming weight is called an isometry from $C_1$ to $C_2$. If $g$ can be extended to an isometry of $A^n$, $C_1$ and $C_2$ are called equivalent. A module $R_A$ is said to have the extension property if every isometry between two codes in $A^n$ can be extended to an isometry of $A^n$. A finite ring $R$ is said to have the extension property if $R_R$ has the property. The MacWilliams extension theorem in coding theory states that finite fields have the extension property.
Lemma 12 (Bass) Let \( R \) be a left or right artinian ring.

(i) If \( A \) is a left ideal of \( R \) and \( r \in R \) such that \( A + Rr = R \), then \( A + r \) contains a unit of \( R \).

(ii) If \( B \) is a right ideal of \( R \) and \( s \in R \) such that \( A + sR = R \), then \( B + s \) contains a unit of \( R \).

A partial order. Let \( R \) be a ring and \( M_R \) a right \( R \)-module. For \( x, y \in M \), define \( x \leq y \) if \( xR \subseteq yR \); define \( x \approx y \) if \( x = yu \) for some \( u \in R^\times \). Then \( \leq \) is a transitive relation and \( \approx \) is an equivalence relation on \( M \). Moreover, \( \leq \) induces a transitive relation, also denoted by \( \leq \), on \( M/\approx \).

Corollary 13 If \( R \) is left or right artinian, then the above relation \( \leq \) on \( M/\approx \) is a partial order.
Cauchy binomial theorem.

\[
\prod_{j=0}^{n} (1 + xq^j) = \sum_{j=0}^{n} \binom{n}{j} q^{\frac{j}{2}} x^j.
\]

**Theorem 14 (J. Wood 07)** Let \( R \) be a finite ring. Then \( R \) is Frobenius \( \iff \) \( R \) has the extension property.

**proof** \((\Rightarrow)\) Let \( C \subset R^n \) be a linear code and let \( f = (f_1, \ldots, f_n) : C \to R^n \) be a weight preserving \( R \)-map. We want to show that \( f \) can be extended to an isometry of \( R^n \). Let \( \pi_i : R^n \to R \) be the \( i \)th projection.

Let \( \chi \) be a generating character of \( R \). \( \forall a \in R \), we have

\[
\sum_{r \in R} e^{2\pi i \chi(ar)} = \begin{cases} |R| & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}
\]

So, \( \forall x \in C \),

\[
\sum_{j=1}^{n} \sum_{r \in R} e^{2\pi i \chi(f_j(x)r)} = |R| |f(x)| = |R| |x| = \sum_{j=1}^{n} \sum_{r \in R} e^{2\pi i \chi(\pi_j(x)r)}.
\]

(5)

For each \( 1 \leq j \leq n \) and \( r \in R \), \( e^{2\pi i \chi(f_j(\cdot)r)} \) and \( e^{2\pi i \chi(\pi_j(\cdot)r)} \) are characters of \( C \). By the orthogonality relation of characters, the terms in the sum at the sum at the LHS
of (5), after a suitable ordering, are the same as the
terms in the sum at the RHS of (5).

The dual module $C^*$ as a right $R$-module has a transitive
relation $\leq$. Among $f_1, \ldots, f_n, \pi_1, \ldots, \pi_n \in C^*$, choose one
say $f_1$ maximal with respect to $\leq$. From the above, we
have $e^{2\pi i \chi(f_i(\cdot))} = e^{2\pi i \chi(\pi_{j_1}(\cdot) r_1)}$ for some $1 \leq j_1 \leq n$ and
$r_1 \in R$. Then $\chi(f_1(\cdot)) = \chi(\pi_{j_1}(\cdot) r_1)$. Thus $\im(f_1 - \pi_{j_1} r_1) \subseteq \ker \chi$. Since $\chi$ is a generating character, we
have $f_1 = \pi_{j_1} r_1$. So $f_1 \leq \pi_{j_1}$. The maximality of $f_1$
implies that $\pi_{j_1} \leq f_1$. By Corollary 13, $f_1 = \pi_{j_1} u_1$ for
some $u_1 \in R^\times$. Since

$$
\sum_{r \in R} e^{2\pi i \chi(f_1(x)r)} = \sum_{r \in R} e^{2\pi i \chi(\pi_{j_1}(x) u_1 r)} = \sum_{r \in R} e^{2\pi i \chi(\pi_{j_1}(x)r)},
$$

Equation (5) is reduced to

$$
\sum_{2 \leq j \leq n} \sum_{r \in R} e^{2\pi i \chi(f_j(x)r)} = \sum_{1 \leq j \leq n} \sum_{r \in R \atop j \neq j_1} e^{2\pi i \chi(\pi_j(x)r)}. \quad (6)
$$

By induction, $\exists$ a permutation $\rho$ of $\{1, \ldots, n\}$ and $u_1, \ldots, u_n \in R^\times$ such that $f_i = \pi_{\rho(i)} u_i$, $1 \leq i \leq n$. Now $(\pi_{\rho(1)} u_1, \ldots, \pi_{\rho(n)} u_n)$
is an isometry of $R^n$ and an extension of $f$. 
(⇐) Assume to that \( R \) is not Frobenius. We want to show that \( R \) does not have the extension property.

1° Write

\[
R/J = M_{n_1}(\mathbb{F}_{q_1}) \times \cdots \times M_{n_k}(\mathbb{F}_{q_k}).
\]

Let \( S_i = M_{n_i \times 1}(\mathbb{F}_{q_i}) \) viewed as a left \( M_{n_i}(\mathbb{F}_{q_i}) \)-module; \( S_i \) is the unique simple \( M_{n_i}(\mathbb{F}_{q_i}) \)-module up to isomorphism. By an observation of Dinh and López-Permouth, we may assume that \((n_1 + 1)S_1 \hookrightarrow_{R} R\). Put \( n = n_1 \) and \( q = q_1 \). Then \((n + 1)S_1 \cong M_{n \times (n+1)}(\mathbb{F}_{q}) \) as \( M_{n}(\mathbb{F}_{q}) \)-module.

2° Let

\[
N = \prod_{i=1}^{n}(1+q^i) = \sum_{0 \leq i \leq n+1} \begin{bmatrix} n + 1 \\ i \end{bmatrix}_q \cdot \left( \sum_{0 \leq i \leq n+1} \begin{bmatrix} n + 1 \\ i \end{bmatrix}_q \right).
\]

Define two \( N \)-tuples \( v_+, v_- \in M_{n+1}(\mathbb{F}_{q})^N \) as follows: The entries of \( v_+ \) are reduced column echelon forms of even rank in \( M_{n+1}(\mathbb{F}_{q}) \); each reduced column echelon form of rank \( 2i \) appears \( q^{\binom{n}{i}} \) times in \( v_+ \). The entries of \( v_- \) are reduced column echelon forms of odd rank in \( M_{n+1}(\mathbb{F}_{q}) \); each reduced column echelon form of rank \( 2i + 1 \) appears \( q^{\binom{n}{2i+1}} \) times in \( v_- \).

Define

\[
C_+ = \{Xv_+ : X \in M_{n \times (n+1)}(\mathbb{F}_{q})\} \subset M_{n \times (n+1)}(\mathbb{F}_{q})^N,
\]

\[
C_- = \{Xv_- : X \in M_{n \times (n+1)}(\mathbb{F}_{q})\} \subset M_{n \times (n+1)}(\mathbb{F}_{q})^N.
\]

19
where $Xv_+$ is the result of multiplying $X$ to each component of $v_+$. Then obviously,

$$f : \ C_+ \rightarrow \ C_- \ \ \ Xv_+ \rightarrow \ Xv_- , \ X \in M_{n \times (n+1)}(\mathbb{F}_q), \ (7)$$

is a well defined $M_n(\mathbb{F}_q)$-isomorphism. We claim that $f$ preserves the Hamming weight. Let $X \in M_{n \times (n+1)}(\mathbb{F}_q)$ with rank $X = r$. Then the number of reduced column echelon forms $Y \in M_{n+1}(\mathbb{F}_q)$ of rank $i$ such that $XY \neq 0$ is $\left[ \begin{array}{c} n+1 \\ i \end{array} \right]_q - \left[ \begin{array}{c} n+1-r \\ i \end{array} \right]_q$. So

$$|Xv_+| - |Xv_-| = \sum_{i=0}^{n+1} (-1)^i q^i \left( \left[ \begin{array}{c} n+1 \\ i \end{array} \right]_q - \left[ \begin{array}{c} n+1-r \\ i \end{array} \right]_q \right) = 0.$$

3° $C_+$ and $C_-$ are not equivalent. $C_+$ has a component $X \cdot 0$ which is always 0; $C_-$ does not have such a component.

4° Using the embedding $M_{n \times (n+1)}(\mathbb{F}_q) \hookrightarrow R^R$, $C_+$ and $C_-$ can be viewed as $R$-submodules of $(R^R)^N$. The map $f$ in (7) is an $R$-isomorphism which preserves the Hamming weight of $(R^R)^N$. We claim that \( \exists \) monomial transformation $h : (R^R)^N \rightarrow (R^R)^N$ such that $h|_{C_+} = f$. Otherwise, $h|_{M_{n \times (n+1)}(\mathbb{F}_q)^N} : M_{n \times (n+1)}(\mathbb{F}_q)^N \rightarrow M_{n \times (n+1)}(\mathbb{F}_q)^N$ would be a monomial transformation whose restriction to $C_+$ is $f$, a contradiction to 3°. Therefore $R$ does not have the extension property.
**Observation** [Dinh and López-Permouth] Let $R$ be a left (or right) artinian ring and let $J = \text{rad } R$ and $\bar{R} = R/J$. Then $\bar{R}$ is semisimple, so

$$\bar{R} \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k),$$

where $n_i > 0$ and $D_i$ is a division ring. Let

$$\epsilon_{ij} = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}_{n_i \times n_i} \in M_{n_i}(D_i).$$

Then $1_{\bar{R}} = \sum_{i,j} \epsilon_{ij}$ is a decomposition of $1_{\bar{R}}$ into primitive orthogonal idempotents with $\epsilon_{ij} \cong \epsilon_{i'j'}$ iff $i = i'$. Let $\epsilon_i = \epsilon_{i1}$. Then $\bar{R}\epsilon_1, \ldots, \bar{R}\epsilon_k$ is the list of all nonisomorphic simple $\bar{R}$ modules. Note that simple $\bar{R}$-modules are precisely simple $R$-modules. We have $R\bar{R} = \bigoplus_{i=1}^k n_i \cdot \bar{R} \epsilon_i$. Write $\text{soc}(R\bar{R}) \cong \bigoplus_{i=1}^k m_i \cdot \bar{R} \epsilon_i$. Then $m_1 + \cdots + m_k \geq n_1 + \cdots + n_k$. (This can be seen by lifting the idempotents $\epsilon_{ij}$ to $R$.) Thus $\text{soc}(R\bar{R}) \cong R\bar{R} \iff m_i \leq n_i$ for all $i$. If $|R| < \infty$, by the note after Theorem 5, $R$ is Frobenius $\iff m_i \leq n_i$ for all $i$. So, if a finite ring $R$ is not Frobenius, then $\exists i$ such that $(n_i+1) \cdot \bar{R} \epsilon_i \hookrightarrow R\bar{R}$. 

20
**Lecture 2. Frobenius Local Rings**

**Finite Frobenius Local Rings**

**Theorem 15** Let $R$ be a finite ring. The following statements are equivalent.

(i) $R$ is Frobenius and local.

(ii) $R$ is QF and local.

(iii) $R$ has a unique minimal left ideal.

(iv) $R$ has a unique minimal right ideal.

Proof. (i) $\Rightarrow$ (ii). Obvious.

(ii) $\Rightarrow$ (iii) and (iv). Since $R$ is local, $R$ has a unique maximal right ideal $M$. Since $R$ is QF, $l(M)$ is the unique minimal left ideal of $R$. So we have (iii). (iv) follows by symmetry.

(iii) $\Rightarrow$ (iv) and (i). By symmetry, we may assume (iii). Let $L$ be the unique minimal left ideal of $R$. Choose a character $\chi$ of $(R, +)$ such that $\chi$ is nontrivial on $L$. Then $\ker \chi$ does not contain any nonzero left ideal of $R$, so $\chi$ is a generating character of $R$. By Theorem 11, $R$ is Frobenius. Since $R$ is QF, $r(L)$ is the unique maximal right ideal of $R$. Thus $R$ is local.
Example. Consider

\[ R = \mathbb{Z}_p m[X]/(X^n, p^a X^{n-1} - p^b), \]

where \( p \) is a prime and \( n \geq 2, 0 \leq a, b \leq m \) are integers.

If \( b \leq a \), then in \( R \),

\[
\begin{align*}
p^b &= p^a X^{n-1} = p^{a-b} X^{n-1} p^b \\
&= p^{a-b} X^{n-1} p^a X^{n-1} = 0.
\end{align*}
\]

Thus \( R \cong \mathbb{Z}_p m[X]/(X^n) \), which is not interesting. \( (R \) has a unique minimal ideal \( p^{b-1} X^{n-1} R. \)

So we assume \( b > a \). Since in \( R \),

\[
\begin{align*}
p^{2b-a} &= p^{b-a} p^b = \\
p^{b-a} p^a X^{n-1} &= p^b X^{n-1} = p^a X^{n-1} X^{n-1} = 0,
\end{align*}
\]

we have \( R \cong \mathbb{Z}_{p^m \min\{m, 2b-a\}} m[X]/(X^n, p^a X^{n-1} - X^b) \). Thus we may assume \( m \leq 2b - a \).

If \( a = 0 \) and \( n = 2 \), then \( X^2 = (X + p^b)(X - p^b) \) in \( \mathbb{Z}_p m[X] \) since \( m \leq 2b - a \leq 2b \). So \( R = \mathbb{Z}_p m[X]/(x^2, X - p^b) \cong \mathbb{Z}_p m[X]/(X - p^b) \cong \mathbb{Z}_p m \).

If \( a = 0 \) and \( b = m \), then \( R = \mathbb{Z}_p m[X]/(X^{n-1}) \), which is also uninteresting.

Therefore, we assume

\( 0 \leq a < b \leq m, \ 2b-a \geq m, \ (a,n) \neq (0,2), \ (a,b) \neq (0,m). \)

We have the following facts.

(i) \( (R, +) \cong \mathbb{Z}_p m \times \mathbb{Z}_p^{n-2} \times \mathbb{Z}_p^m \).

(ii) \( R \) is Frobenius and local \( \iff 2b-a = m \). When \( 2b-a = m \), \( p^{m-1} R \) is the unique minimal ideal of \( R. \)
Lemma 16 (A variation of Hensel’s lemma)

Let $R$ be a commutative ring, $m$ a nilpotent ideal of $R$, and $k = R/m$. Let $(\ ) : R \to k$ be the natural homomorphism. Let $f, g \in k[x]$ such that $f$ is monic and $f, g$ are coprime. Let $H \in R[x]$ such that $\bar{H} = fg$. Put

$$A = \{ F \in R[x] : F \text{ is monic and } \bar{F} = f \},$$
$$B = \{ L \in m[x] : \deg L < \deg f \}$$

and define

$$\phi : A \longrightarrow B$$
$$F \longmapsto L,$$

where $L$ is given by the Euclidean algorithm

$$H = GF + L, \quad G, L \in R[x], \quad \deg L < \deg F.$$ 

Then $\phi$ is a bijection. In particular, $\exists! F, G \in R[x]$ such that $F$ is monic, $\bar{F} = f$, $\bar{G} = g$ and $H = FG$. 

23
Basic polynomials. Let $p$ be a prime and $n \in \mathbb{Z}^+$. The homomorphism $\overline{\ )} : \mathbb{Z}_{p^n} \to \mathbb{Z}_p$ induces a homomorphism $\mathbb{Z}_{p^n}[x] \to \mathbb{Z}_p[x]$. A monic polynomial $f \in \mathbb{Z}_{p^n}[x]$ is called basic if its image $\bar{f} \in \mathbb{Z}_p[x]$ is irreducible.

Lemma 17 If $f_1, f_2 \in \mathbb{Z}_{p^n}[x]$ are two basic polynomials of the same degree, then $\mathbb{Z}_{p^n}[x]/(f_1) \simeq \mathbb{Z}_{p^n}[x]/(f_2)$.

Proof. Let $R = \mathbb{Z}_{p^n}[x]/(f_1)$ and $k = R/pR$. Then $k = \mathbb{F}_{p^t}$, where $t = \deg f_1$. Since $\bar{f}_2 \in \mathbb{Z}_p[x]$ has degree $t$, $\bar{f}_2$ has a zero $\alpha \in k$, so $\bar{f}_2 = (x - \alpha)g$ for some $g \in k[x]$. By Lemma 16, $f_2 = (x - a)G$ for some $a \in R$ with $\bar{a} = \alpha$ and some $G \in R[x]$.

We claim that $R = \mathbb{Z}_{p^n}[a]$. For each $b \in R$, since $\bar{b} \in k = \mathbb{Z}_p[\alpha]$, we have $\bar{b} = h_0(\alpha)$ for some $h_0 \in \mathbb{Z}_p[x]$. Choose $H_0 \in \mathbb{Z}_{p^n}[x]$ such that $\bar{H}_0 = h_0$. Then $\bar{b} = \bar{H}_0(a)$, so $b = H_0(a) + pb_1$ for some $b_1 \in R$. By induction and the fact that $p^n = 0$ in $R$, we have $b = H_0(a) + pH_1(a) + \cdots + p^{n-1}H_{n-1}(a)$ for some $H_0, \ldots, H_{n-1} \in \mathbb{Z}_{p^n}[x]$. So $b \in \mathbb{Z}_{p^n}[a]$ and the claim is proved.

Now the ring homomorphism
\[
\phi : \mathbb{Z}_{p^n}[x] \rightarrow R \\
f \mapsto f(a)
\]
induces an onto homomorphism $\overline{\phi} : \mathbb{Z}_{p^n}[x]/(f_2) \rightarrow R$. Since $|\mathbb{Z}_{p^n}[x]/(f_2)| = p^{nt} = |R|$, $\overline{\phi}$ is an isomorphism.
**Galois rings.** Let \( f \in \mathbb{Z}_p^n[x] \) be a basic polynomial of degree \( t \). The ring \( \mathbb{Z}_p^n[x]/(f) \), which depends only on \( p, n, t \), is called the Galois ring and is denoted by \( \text{GR}(p^n, t) \).

- \( (\text{GR}(p^n, t), +) = \mathbb{Z}_{p^n}^t \).

- \( \text{GR}(p^n, t) \) is a commutative local ring with maximal ideal \((p)\) and residue field
  \( \text{GR}(p^n, t)/(p) = \mathbb{F}_{p^t} \).

- All ideals of \( \text{GR}(p^n, t) \) are \( \text{GR}(p^n, t) = (p^0) \supset (p^1) \supset \cdots \supset (p^n) = 0 \). Thus \( \text{GR}(p^n, t) \) is a finite commutative Frobenius local ring with a unique minimal ideal \((p^{n-1})\).
Teichmüller set. Let \( f \in \mathbb{Z}_p[x] \) be a monic primitive irreducible polynomial of degree \( t \). Then \( f \mid x^{p^t-1} - 1 \) in \( \mathbb{Z}_p[x] \). By Lemma 16, \( \exists \) basic polynomial \( F \in \mathbb{Z}_{p^n}[x] \) such that \( \bar{F} = f \) and \( F \mid x^{p^t-1} - 1 \) in \( \mathbb{Z}_{p^n}[x] \). We have

\[
\text{GR}(p^n, t) = \mathbb{Z}_{p^n}[x]/(F) = \mathbb{Z}_{p^n}[\omega],
\]

where \( \omega \) is the image of \( x \) in \( \mathbb{Z}_{p^n}[x]/(F) \). \( \bar{\omega} \in \text{GR}(p^n, t)/(p) = \mathbb{F}_{p^t} \) is a root of \( f \). Hence the multiplicative order \( o(\bar{\omega}) = p^t - 1 \). Thus \( o(\omega) = p^t - 1 \). The set \( T = \{0, 1, \omega, \ldots, \omega^{p^t-2}\} \) is called the Teichmüller set of \( \text{GR}(p^n, t) \). Since \( \bar{0}, \bar{1}, \bar{\omega}, \ldots, \bar{\omega}^{p^t-2} \) are all distinct in \( \mathbb{F}_{p^t} \), \( T \) is a set of representatives of cosets of \( (p) \) in \( \text{GR}(p^n, t) \).

The elements

\[
\xi_0 + p\xi_1 + \cdots + p^{n-1}\xi_{n-1}, \quad \xi_i \in T \quad (8)
\]

are all distinct for different \( (\xi_0, \ldots, \xi_{n-1}) \). Thus every element in \( \text{GR}(p^n, t) \) can be uniquely expressed in the form (8), which is called the \( p \)-adic expansion of the element.
Multiplicative group. Using the $p$-adic expansion (8), we see that the multiplicative group of $\text{GR}(p^n, t)$ is

$$\text{GR}(p^n, t)^\times = T^\times (1 + p\text{GR}(p^n, t)) \cong T^\times \times (1 + p\text{GR}(p^n, t)),$$

where $T^\times = T \setminus \{0\} = \langle \omega \rangle \cong \mathbb{Z}_{p^t-1}$. Since $|\text{GR}(p^n, t)^\times| = (p^t-1)p^{(n-1)t}$, $T^\times$ is the only cyclic subgroup of $\text{GR}(p^n, t)^\times$ of order $p^t - 1$. It follows that the Teichmüller set of $\text{GR}(p^n, t)$ is unique. In (9), it can be shown that

$$1 + p\text{GR}(p^n, t) \cong \begin{cases} 
\mathbb{Z}_{p^{n-1}} & \text{if } p \text{ is odd or } p = 2 \text{ and } n \leq 2, \\
\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_{2^{n-1}} & \text{if } p = 2 \text{ and } n \geq 3.
\end{cases}$$

Automorphism group.

**Proposition 18** Define

$$\sigma: \text{GR}(p^n, t) \rightarrow \text{GR}(p^n, t)$$

$$\sum_{i=0}^{n-1} \xi_i p^i \mapsto \sum_{i=0}^{n-1} \xi_i^p p^i, \quad \xi_i \in T.$$  \hspace{1cm} (10)

Then $\sigma \in \text{Aut}(\text{GR}(p^n, t))$, $o(\sigma) = t$ and $\text{Aut}(\text{GR}(p^n, t)) = \langle \sigma \rangle$. $\sigma$ is called the Frobenius map of $\text{GR}(p^n, t)$.
**Theorem 19** Let $R = \text{GR}(p^n, r)$ and let $\sigma$ be the Frobenius automorphism of $R$. Let $R^M_R$ be an $(R, R)$-bimodule. Then

$$R^M_R = M_1 \oplus \cdots \oplus M_r \quad (\text{as } (R, R)\text{-bimodule}),$$

where

$$xa = \sigma^i(a)x \quad \forall x \in M_i, \ a \in R.$$
Finite Chain Rings

A finite chain ring is a finite ring whose left ideals form a chain under inclusion. This definition is left-right symmetric. (Since a finite chain ring $R$ is QF, $A \mapsto r(A)$ is an inclusion reversing bijection from the set of all left ideals of $R$ to the set of all right ideals of $R$.) The structure of finite chain rings was determined by Clark and Drake (1973). Let $R$ be a finite chain ring with maximal ideal $M$. The following steps lead us to a concrete description of $R$.

1° $M = R\pi$ for some $\pi \in R$. Write $M = Ra_1 + \cdots + Ra_n$, $a_i \in M$. Since $Ra_1, \ldots, Ra_n$ form a chain, $M = Ra_i$ for some $i$.

2° Since $M$ is the unique maximal left ideal of $R$, $M = \text{rad } R$. So $M$ is an ideal of $R$. Moreover, $\pi$ is nilpotent. Let $s$ be the nilpotency of $\pi$. We claim that for $0 \leq i \leq s - 1$, $\pi^i \notin R\pi^{i+1}$. Otherwise, $\pi = r\pi^{i+1}$ for some $r \in R$, i.e., $\pi^i(1 - r\pi) = 0$. Since $1 - r\pi$ is invertible, $\pi^i = 0$, which is a contradiction. In the same way, $\pi^i \notin \pi^{i+1}R$.

3° For each $0 \leq i \leq s - 1$, $R\pi^i/R\pi^{i+1} \cong R/R\pi$.  

29
Define \( f : R/R\pi \to R\pi^i/R\pi^{i+1}, r + R\pi \mapsto r\pi^i + R\pi^{i+1} \). Then \( f \) is an onto \( R \)-map. By \( 2^\circ \), \( R\pi^i/R\pi^{i+1} \neq 0 \). Since \( R/R\pi \) is simple, \( f \) is onto.

4° Since \( R/R\pi \) is a simple \( R \)-module, by \( 3^\circ \),
\[
R = R\pi^0 \supset R\pi^1 \supset \cdots \supset R\pi^s = 0
\]
are all left ideals of \( R \). Let \( R/R\pi = \mathbb{F}_p \). Then \(|R\pi^i/R\pi^{i+1}| = p^r\), \( 0 \leq i \leq s - 1 \), so \(|R\pi^i| = p^{(s-i)r} \).

5° Since \( R\pi \) is a two-sided ideal of \( R \), all \( R\pi^i \) are two-sided ideal of \( R \). By \( 2^\circ \), \( R = \pi^0 R \supset \pi^1 R \supset \cdots \supset \pi^s R = 0 \). Since \( R \) is QF, it has precisely \( s + 1 \) right ideals. So we must have \( \pi^i R = R\pi^i, 0 \leq i \leq s \).

6° Let \( \text{char } R = p^n \), then \( R \) contains a copy of \( GR(p^n, r) \).

We first show that \( \exists \omega \in R^\times \) such that \( o(\omega) = p^n - 1 \). Choose \( \omega_1 \in R \) such that its image \( \bar{\omega}_1 \in R/R\pi = \mathbb{F}_p \) has order \( p^t - 1 \). Then \( \omega_1^{p^t - 1} = 1 + r\pi \) for some \( r \in R \). Choose \( u \in \mathbb{Z}^+ \) large enough such that \( \left( \frac{p^n}{i} \right) \equiv 0 \pmod{p^n} \) for all \( 1 \leq i \leq s \). Then \( \omega_1^{(p^t - 1)p^n} = (1 + r\pi)^{p^n} = 1 + \sum_{i=1}^{p^n} \binom{p^n}{i} (r\pi)^i = 1 \). Let \( \omega = \omega_1^{p^n} \).

\( \mathbb{Z}_{p^n}[\omega] \) is a subring of \( R \). So \( \mathbb{Z}_{p^n}[\omega] \) is a commutative local ring. (In general, a subring of a finite local ring \( R \) is local. \( \forall a \in S \setminus S \cap (\text{rad } R), a \in R^\times \). Since \( |R^\times| < \infty \), \( a^m = 1 \) for some \( m > 1 \). Then \( a \in S^\times \).) Let \( m \) be the maximal ideal of \( \mathbb{Z}_{p^n}[\omega] \). Let \( \bar{\omega} \in \mathbb{Z}_{p^n}[\omega]/m \) be the image of \( \omega \). Let \( f \in \mathbb{Z}_p[x] \) be the minimal polynomial of \( \bar{\omega} \) over \( \mathbb{Z}_p \).
Since \( f \mid x^{p^t-1} - 1 \), by Lemma 16, \( \exists \) a basic polynomial \( F \in \mathbb{Z}_p[x] \) such that \( \overline{F} = f \) and \( x^{p^t-1} - 1 = FG \) for some \( G \in \mathbb{Z}_p[x] \). Since \( \overline{F}(\bar{\omega}) = 0 \), we have \( \overline{G}(\bar{\omega}) \neq 0 \) (since \( x^{p^t-1} - 1 \) is separable.) Thus \( G(\omega) \) is invertible in \( \mathbb{Z}_p[\omega] \). Since \( 0 = \omega^{p^t-1} - 1 = F(\omega)G(\omega) \), we have \( F(\omega) = 0 \). Let

\[
\phi : \text{GR}(p^n, r) = \mathbb{Z}_p[x]/(F) \rightarrow \mathbb{Z}_p[\omega]
\]

be the ring homomorphism mapping \( x + (F) \) to \( \omega \). \( \phi \) induces an isomorphism \( \text{GR}(p^n, r)/(p^m) \rightarrow \mathbb{Z}_p[\omega] \) for some \( 1 \leq m \leq n \). (Note that every ideal of \( \text{GR}(p^n, r) \) is of the form \( (p^m) \).) Since \( p^m = \text{char} \text{GR}(p^n, r)/(p^m) = \text{char} \mathbb{Z}_p[\omega] = p^n \), we must have \( m = n \). Thus \( \text{GR}(p^n, r) \cong \mathbb{Z}_p[\omega] \).

7° Let \( S \subset R \) be an isomorphic copy of \( \text{GR}(p^n, r) \). \( \pi \)-adic expansion. The embedding \( S/pS \hookrightarrow R/R\pi \) is an isomorphism since both fields are \( \mathbb{F}_p \). Let \( T \) be the Teichmüller set of \( S \). Then \( T \) is a set of representatives of cosets of \( R\pi \) in \( R \). By induction, every element of \( R \) can be uniquely written as

\[
\xi_0 + \xi_1\pi + \cdots + \xi_{s-1}\pi^{s-1}, \quad \xi_i \in T.
\]

(11)

8° Since \( M \) is an \((S, S)\)-bimodule, by the above theorem,

\[
sM_S = M_1 \oplus \cdots \oplus M_r \quad \text{(as \((S, S)\)-bimodule)},
\]

where

\[
xa = \sigma^i(a)x \quad \forall x \in M_i, \ a \in S.
\]
\[ \exists M_i \not\subset M^2. \] So we may choose \( \pi \) in \( 1^o \) such that \( \pi \in M_i. \) Then

\[ \pi a = \sigma^i(a) \pi \quad \forall a \in S. \]

9\(^o\) Let \( e \leq s \) be the largest integer such that \( p \in R\pi^e. \) Then \( p = u\pi^e \) for some \( u \in R^x. \) Thus \( \pi^{ne} = u^{-n}p^n = 0 \) but \( \pi^{(n-1)e} = u^{-(n-1)}p^{n-1} \neq 0. \) So \((n - 1)e < s \leq ne.\)

Write

\[ s = (n - 1)e + t, \quad 1 \leq t \leq e. \]

Note that if \( n = 1, \) then \( s = t \) and by definition, \( e = s = t. \) We claim that

\[ sR = S \oplus S\pi \oplus \cdots \oplus S\pi^{k-1} \quad (12) \]

and

\[ s(S\pi^i) \cong \begin{cases} S & \text{if } 0 \leq i \leq t - 1, \\ S/p^{n-1}S \cong Sp & \text{if } t \leq i \leq k - 1. \end{cases} \quad (13) \]

Define \( f : S \rightarrow S\pi^i, \ a \mapsto a\pi^i. \) Then clearly,

\[ \ker f = \begin{cases} 0 & \text{if } 0 \leq i \leq t - 1, \\ p^{n-1}S & \text{if } t \leq i \leq e - 1. \end{cases} \]

So we have the isomorphism in (13).

By (12) we have

\[ sR = S + S\pi + \cdots + S\pi^{s-1} \]

\[ = S + S\pi + \cdots + S\pi^{e-1} + Rp. \]

\[ \text{(14)} \]
By Nakayama’s lemma,
\[ SR = S + S\pi + \cdots + S\pi^{s-1}. \]  
(15)

By (13),
\[ |S| = |S\pi| \cdots |S\pi^{s-1}| = |S|^t |S\pi|^{e-t} = p^{\frac{p}{r}t} p^{(n-1)r(e-t)} = p^{\frac{r}{r}(n-1)^e+t} = p^r = |R|. \]

So the sum in (15) is direct.

10° Since \( \pi^e \in pR \), by 9°,
\[ \pi^e = p(a_{e-1}\pi^{e-1} + \cdots + a_1\pi + a_0), \quad a_i \in S. \]  
(16)

If \( k < s \), we must have \( a_0 \in S^x \) since \( p = u\pi^e, u \in R^x \). If \( e = s \), then \( \pi^e = 0 = p \) and we can choose \( a_0 = 1 \in S \). Thus in (16), we can always choose \( a_0 \in S^x \).

Let \( S[X; \sigma^i] \) be the skew polynomial ring. (In \( S[X; \sigma^i] \), \( aX = X\sigma^i(a) \forall a \in S \).)

Define
\[ f : S[X; \sigma^i] \longrightarrow R \]
\[ a_0 + \cdots + a_m x^m \longmapsto a_0 + \cdots + a_m \pi^m. \]

Clearly, \( f \) is an onto homomorphism. We claim that
\[ \ker f = (g, p^{n-1}X^t), \]
where \( g = X^e - p(a_{e-1}X^{e-1} + \cdots + a_0) \). Clearly, \( (g, p^{n-1}X^t) \subset \ker f \). Suppose \( h \in \ker f \). We may assume \( \deg h \leq e - 1 \) because of \( g \). Write \( h = \alpha_0 + \cdots + \alpha_{e-1}X^{e-1}, \alpha_i \in S \). Then \( \alpha_0 + \cdots + \alpha_{e-1}X^{e-1} = 0 \). By (12), \( \alpha_i\pi^i = 0 \) for all
0 \leq i \leq e, which implies that \( \alpha_0 = \cdots = \alpha_{t-1} = 0 \) and 
\( \alpha_t, \ldots, \alpha_{e-1} \in p^{n-1}S. \) So \( h \in (g, p^{n-1}X^t). \)

Now we arrive at the conclusion that

\[
R \cong S[X; \sigma^i]/(g, p^{n-1}X^t).
\]
Facts about finite chain rings. Here is a summary of properties of finite chain rings.

- Every finite chain ring $R$ is of the form

$$R \cong S[X; \alpha]/(g, p^{n-1}X^t),$$

where $p$ is a prime, $n \geq 1$, $S = GR(p^n, r)$, $\alpha \in \text{Aut}(S)$, $g = X^e - p(a_{e-1}X^{e-1} + \cdots + a_0) \in S[X; \alpha]$, $a_i \in S$, $a_0 \in S^\times$, $t = e$ if $n = 1$ and $1 \leq t \leq e$ if $n > 1$. Let $\pi$ be the image of $X$ in $R$. Then $\text{rad} R = R\pi$, $R/R\pi = \mathbb{F}_{p^r}$, $Rp = R\pi^k$, and the nilpotency of $\pi$ is $(n-1)e + t$. We call $R$ in (17) a finite chain ring of type $(p, n, r, k, t)$.

- $(R, +) \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^{e-t}}$.

- Let $T^\times$ be the cyclic subgroup of $S^\times$. (Note that $S \hookrightarrow R$.) Then

$$R^\times = T^\times(1 + R\pi) = T^\times \ltimes (1 + R\pi).$$

The structure of $R^\times$ is not known in general.

- $\text{Aut}(R) = ?$. 

Finite Commutative Chain Rings

Let $p$ be a prime and let $n, r, e, t$ be positive integers such that $t = e$ if $n = 1$ and $1 \leq t \leq e$ if $n > 1$. It follows from (17) that every finite commutative chain ring of type $(p, n, r, e, t)$ is of the form

$$R = S[X]/(g, p^{n-1}X^t),$$

(18)

where $S = GR(p^n, r)$, $g = X^e - p(a_{e-1}X^{e-1} + \cdots + a_0) \in S[X]$, $a_i \in S$, $a_0 \in S^\times$.

**Multiplicative group.** We have

$$R^\times = T^\times(1 + R\pi) = T^\times \times (1 + R\pi).$$

$T^\times$ is the unique cyclic subgroup of $R^\times$ of order $p^r - 1$. $1 + R\pi$ is a finite abelian $p$-group. In most cases, the structure of $1 + R\pi$ is completely determined by the type $(p, n, r, e, t)$ (Theorems 20, T2.8). There is a remaining case where the structure of $1 + R\pi$ depends not only on the type $(p, n, r, e, t)$ but also on the Eisenstein polynomial $g$. The result in this case is less explicit (Theorem 22).
Theorem 20 (H-L-M 03) Let $R$ be a finite commutative chain ring of type $(p, 1, r, e, t)$, i.e., $R = \mathbb{F}_{p^r}[X]/(X^e)$. Let $I = \{i \in \mathbb{Z} : 1 \leq i < e, \ p \nmid i\}$. Then

$$1 + R\pi \cong \bigoplus_{i \in I} \mathbb{Z}_{r\left\lfloor \log_p \frac{p}{i} \right\rfloor}.$$ 

Theorem 21 (H-L-M 03) Let $n > 1$ and let $R$ be a finite commutative chain ring of type $(p, n, r, e, t)$ given by (18). Assume that either $(p-1) \nmid e$ or $(p-1) | e$ but the image of $-a_0$ in $R/R\pi = \mathbb{F}_p$ is not a $(p-1)$st power. Let $s = (n-1)e + t$ and

$$I = \left\{i \in \mathbb{Z} : 1 \leq i \leq \min\left\{s, \frac{pe}{p-1}\right\}, \ p \nmid i\right\}. \quad (19)$$

For each $i > 0$, let

$$\iota(i) = \max\left\{0, \left\lfloor \log_p \frac{k}{(p-1)i} \right\rfloor\right\},$$

$$\alpha(i) = \iota(i) + \left\lfloor \frac{s - ip^{\iota(i)}}{e} \right\rfloor.$$ 

Then

$$1 + R\pi \cong \bigoplus_{i \in I} \mathbb{Z}_{r}^{\alpha(i)}.$$
Theorem 22 (H-L-M 03) Let \( n > 1 \) and let \( R \) be a finite commutative chain ring of type \((p, n, r, e, t)\) given by (18). Assume that \( e = c(p - 1)p^u, \ p \nmid c, \ u \geq 0 \) and that the image of \(-a_0\) in \( R/R\pi = \mathbb{F}_{p^r} \) is a \((p - 1)\)st power. Let \( \psi : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}, \ z \mapsto z^{p^u} + \bar{a}_0 z^{p^u+1} \). Choose \( \epsilon - 1, \ldots, \epsilon_r \in R \) such that their images \( \bar{\epsilon}_1, \ldots, \bar{\epsilon}_r \in R/R\pi = \mathbb{F}_{p^r} \) form a basis of \( \mathbb{F}_{p^r} \) over \( \mathbb{F}_p \) and \( \ker \psi = \langle \bar{\epsilon}_r \rangle \). Choose \( \delta \in R \) such that \( \psi(\bar{\epsilon}_1), \ldots, \psi(\bar{\epsilon}_r-1), \bar{\delta} \) form a basis of \( \mathbb{F}_{p^r} \) over \( \mathbb{F}_p \). Then \( \exists \gamma \in \mathbb{Z} \) and \( \gamma(i, j) \in \mathbb{Z} \) for each \((i, j) \in \Omega \) such that

\[
(1+\pi^c\epsilon_r)^{p^u+1} = (1+\pi^{cp^u+1}\delta)^{\gamma} \prod_{(i, j) \in \Omega} (1+\pi^{i\epsilon_j})^{\gamma(i, j)}. \tag{20}
\]

\( 1 + R\pi \) is the abelian \( p \)-group with generators \( x_{i,j} \ (i \in I, \ 1 \leq j \leq r) \) and \( x \) subject to the relations

\[
\begin{cases}
x_{i,j}^{p^{\alpha(i)}} = 1, & (i, j) \in \Omega, \\
x_{i,j}^{p^{\alpha(p^u+1)}} = 1, \\
x_{cr}^{p^{u+1}} = x^\gamma \prod_{(i, j) \in \Omega} x_{i,j}^{\gamma(i, j)}.
\end{cases}
\]
Finite commutative chain rings and $p$-adic fields. Let $\mathbb{Q}_p$ be the field of $p$-adic numbers and let $\mathbb{Z}_p$ denote the ring of $p$-adic integers. (Since we use $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$, the notation for the ring of $p$-adic integers needs to be a little different from $\mathbb{Z}_p$.)

Let $K/\mathbb{Q}_p$ be a finite extension, with residue degree $f$ and ramification index $e$. Let $o_K$ be the ring of integers of $K$, $\pi_K$ a prime of $K$, and $\bar{K} = o_K/\pi_K o_K$ the residue field of $K$. Let $k/\mathbb{Q}_p$ be the maximal unramified subextension of $K/\mathbb{Q}_p$. Let $s, t, n$ be positive integers such that $s = (n - 1)e + t$, where $1 \leq t \leq e$.

Choose $a \in o_k$ be such that $\bar{k} = \mathbb{Z}_p[\bar{a}]$, where $\bar{a}$ is the image of $a$ in $\bar{k}$. Let $\Phi \in \mathbb{Z}_p[X]$ be the minimal polynomial of $a$ over $\mathbb{Q}_p$. Then the image $\bar{\Phi}$ of $\Phi$ in $(\mathbb{Z}_p/p^n\mathbb{Z}_p)[X] = \mathbb{Z}_{p^n}[X]$ is a basic of degree $r$ and

$$o_k/p^n o_k \cong \mathbb{Z}_{p^n}[X]/(\bar{\Phi}) \cong \text{GR}(p^n, r).$$

The minimal polynomial of $\pi_K$ over $k$ is an Eisenstein polynomial $\Psi \in o_k[X]$ of degree $e$ such that

$$o_K/\pi_K^s o_K \cong (o_k/p^n o_k)[X]/(\bar{\Psi}, p^{n-1} X^t) \cong \text{GR}(p^n, f)[X]/(\bar{\Psi}, p^{n-1} X^t),$$

where $\bar{\Psi}$ is the image of $\Psi$ in $(o_k/p^n o_k)[X] \cong \text{GR}(p^n, r)[X]$. $\bar{\Psi}$ is an Eisenstein polynomial over $\text{GR}(p^n, r)$. Thus $o_K/\pi_K^s o_K$ is a finite commutative chain ring with invariants

$$\begin{cases} (p, 1, r, t, t) & \text{if } n = 1, \\ (p, n, r, e, t) & \text{if } n > 1. \end{cases}$$

(21)
Enumeration of isomorphism classes. Let \( C(p, n, r, e, t) \) be the number of isomorphism classes of finite commutative chain rings type \((p, n, r, e, t)\) and let \( I(\mathbb{Q}_p, f, e) \) denote the number of isomorphism classes of finite extensions \( K/\mathbb{Q}_p \) with residue degree \( r \) and ramification index \( e \).

\[
C(p, n, r, e, t) = I(\mathbb{Q}_p, f, e)
\]

when

\[
(n - 1)e + t > \left(\frac{p}{p - 1} + \nu_p(e)\right)e.
\]

The number \( C(p, n, f, e, t) \) is difficult to compute when \( \nu_p(e) > 0 \). In certain cases, explicit formulas for \( C(p, n, r, e, t) \) are known; these formulas are given in the following theorems. (When \( n = 1 \), obviously, \( C(p, n, r, e, t) = 1 \). So we assume \( n > 1 \).)
Theorem 23 (Clark and Liang 73 and Hou 01)

Let \( p \) be a prime and let \( n, f, e, t \) be positive integers such that \( n \geq 2, 1 \leq t \leq e, \) and \( p \nmid e. \)

Then

\[
\mathcal{C}(p, n, f, e, t) = \sum_{c \mid (e, p^f-1)} \frac{\phi(c)}{\tau(c)} = \frac{1}{f} \sum_{i=0}^{f-1} \left( p^{(i,f)} - 1, e \right),
\]

(22)

where \( \phi \) is the Euler function, \( (a, b) \) is the greatest common divisor of \( a \) and \( b, \) and \( \tau(c) \) is the smallest positive integer \( m \) such that \( p^m \equiv 1 \pmod{c}. \)
Theorem 24 (Hou-Keating 04) Assume $p \parallel e$ and $n > 3 + \frac{1}{p-1} - \frac{t}{e}$. Let $e_0 = e/p$. Then

$$C(p, n, r, e, t) =$$

$$\frac{1}{re} \sum_{h=0}^{e_0-1} \left( -\frac{p^2br}{c_h} + \sum_{i=0}^{b-1} \sum_{j=0}^{c_h-1} (p^2 + \omega_{hij})p^{\epsilon_{of}(h,i,j)} \right),$$

where

(i) $b = (e_0, p^r - 1)$,

(ii) $c_h$ is the smallest positive integer such that $b \mid (p^{c_h} - 1)_h$

(ii)

$$t(h, i, j) = \begin{cases} \frac{p^{\lcm(r, c_h)}}{p^h-1} - 1 \cdot i + \frac{u^{h_{c_h,j}}}{(r, c_h)} & \text{if } j > 0, \\ i & \text{if } j = 0, \end{cases}$$

where $u \in \mathbb{Z}$ satisfies $e_0u \equiv b \pmod{p^r - 1}$,

(iv) $\omega(h, i, j) = \frac{r}{(r, c_h)} \cdot \frac{b}{(b, t(h,i,j))}$,

(v)

$$\omega_{hij} = \begin{cases} p^2 & \text{if } (p - 1) \mid e, -h \equiv \frac{p^r - 1}{p-1} \pmod{(p - 1)}, \text{ and} \\ \frac{e_0i}{b} + \frac{(p^{h_{c_h,j}} - 1)h}{b} \cdot \frac{e_0u - b}{p - 1} \equiv \frac{p^{h_{c_h,j}} - 1}{p - 1} \pmod{(p - 1)}, \\ p & \text{otherwise.} \end{cases}$$
Theorem 25 (Hou-Keating 04) Assume $p > 2$, $p^2 \parallel e$, $n > 4 + \frac{1}{p-1} - \frac{t}{e'}$, and $(p^f - 1, e) = 1$. Let $e_0 = e/p^2$.

Write $r = p^ir'$ with $p \nmid r'$. Then

$$C(p, n, r, e, t) = \frac{1}{p^ir'} \sum_{\tau | r'} \phi(\tau) \left[ \frac{1}{2}(p - 1, \tau)^2 \frac{(p_{\tau}^r p_{\tau}^i e_0 - 1)^2}{p - 1} ight. $$

$$- (p - 1, \tau)^2 \frac{p_{\tau}^r p_{\tau}^i e_0 (p_{\tau}^r p_{\tau}^i e_0 - 1)}{p - 1} + \frac{1}{2}(p^2 - 1, \tau) \frac{(p_{\tau}^r 2p_{\tau}^i e_0 - 1)}{p - 1} $$

$$+ (p + 1) \left[(p^2 + \frac{\tau}{p} (p+1)p^i e_0 - p_{\tau}^r p_{\tau}^i e_0) - (p^2 - 1)p_{\tau}^r p_{\tau}^i e_0 + p_{\tau}^r 2p_{\tau}^i e_0 \right. $$

$$+ \sum_{j=1}^{i} p^j \left[ \frac{(p_{\tau}^r p_{\tau}^i e_0 - 1)(p_{\tau}^r p_{\tau}^i e_0 - 1 - 1)}{p + 1} \right. $$

$$+ (p - 1)(-p^2 + \frac{\tau}{p} p_{\tau}^i e_0 + p_{\tau}^r p_{\tau}^i e_0 + p_{\tau}^r 2p_{\tau}^i e_0) $$

$$+ (p^2 - 1)(p^2 + \frac{\tau}{p} (p+1)p^i e_0 - p_{\tau}^r p_{\tau}^i e_0) $$

$$\left. + \frac{1}{2}(p - 1, \tau)^2 (p_{\tau}^r p_{\tau}^i e_0 - 1)^2 + \frac{1}{2}(p^2 - 1, \tau)(p_{\tau}^r 2p_{\tau}^i e_0 - 1) \right] \right] .$$
Lecture 3. Partial Difference Sets

An Introduction to Partial Difference Sets

Let $G$ be a finite group. A partial difference set (PDS) in $G$ is a subset $D \subset G$ such that the differences $d_1 d_2^{-1}$ ($d_1, d_2 \in D$, $d_1 \neq d_2$) represent each element in $D \setminus \{e\}$ exactly $\lambda$ times and each element in $G \setminus (D \cup \{e\})$ exactly $\mu$ times. The integers $(v = |G|, k = |D|, \lambda, \mu)$ are called the parameters of the PDS. When $\lambda = \mu$, the PDS is called a difference set.

**Example 26 (Paley PDS)** Let $q$ be a prime power such that $q \equiv 1 \pmod{4}$. Let $D$ be the set of nonzero squares in $\mathbb{F}_q$. Then $D$ is a $(q, \frac{1}{2}(q - 1), \frac{1}{4}(q - 5), \frac{1}{4}(q - 1))$ PDS.
Example 27 (PCP) Let $G$ be a group of order $n^2$. An $(n,r)$ partial congruence partition (PCP) of $G$ is a set $\mathcal{P}$ of $r$ subgroups of order $n$ of $G$ such that if $H_1, H_2 \in \mathcal{P}$ with $H_1 \neq H_2$, then $H_1 \cap H_2 = \{e\}$.

Claim. If $\mathcal{P}$ is an $(n,r)$ PCP of $G$, then $D = \bigcup_{H \in \mathcal{P}}(H \setminus \{e\})$ is a $(n^2, r(n-1), n + r^2 - 3r, r^2 - r)$ PDS in $G$.

Proof. Let $\mathcal{P} = \{H_1, \ldots, H_r\}$. Note that if $i \neq j$, then $H_i \times H_j \rightarrow G, (a,b) \mapsto ab^{-1}$ is a bijection. Let $x \in G \setminus \{e\}$. If $x \notin D$, then for each pair $i \neq j$, $\exists!(a,b) \in (H_i \setminus \{e\}) \times (H_j \setminus \{e\})$ such that $ab^{-1} = x$. So $ab^{-1} = x$ has $r(r-1)$ solutions $(a,b) \in D \times D$. Assume $x \in D$, say $x \in H_1$. Then for each pair $i \neq j$ with $i,j \neq 1$, $\exists!(a,b) \in (H_i \setminus \{e\}) \times (H_j \setminus \{e\})$ such that $ab^{-1} = x$. If exactly one of $i,j$ is 1, Then $\exists!(a,b) \in (H_1 \setminus \{e\}) \times (H_1 \setminus \{e\})$ such that $ab^{-1} = x$. Also $\exists n-2$ pairs $(a,b) \in (H_1 \setminus \{e\}) \times (H_1 \setminus \{e\})$ such that $ab^{-1} = x$. So $ab^{-1} = x$ has $(r-1)(r-2) + n - 2 = n + r^2 - 3r$ solutions $(a,b) \in D \times D$.

An example of PCP. Let $G = \mathbb{F}_q^2$. Any collection of 1-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^2$ is a PCP.
**PDS and strongly regular graphs.** A graph $\Gamma$ with $v$ vertices is called a $(v, k, \lambda, \mu)$ **strongly regular** graph if it has the following properties.

(i) Every vertex belongs to $k$ edges.

(ii) If two vertices are adjacent, there are $\lambda$ additional vertices adjacent to both of them; if two vertices are not adjacent, there are $\mu$ additional vertices adjacent to both of them.

Strongly regular graphs are precisely association schemes with two classes.

Let $G$ be a finite group and $D \subset G \setminus \{e\}$ such that $D^{(-1)} = D$. The Cayley graph $\Gamma(G, D)$ of $D$ has vertex set $G$ such that $a, b \in G$ are adjacent iff $ab^{-1} \in D$. $\Gamma(G, D)$ admits $G$ as a regular automorphism group.

**Fact.** The Cayley graph of $D \subset G$ is a $(v, k, \lambda, \mu)$ strongly regular graph iff $D$ is a $(v, k, \lambda, \mu)$ PDS with $D^{(-1)} = D$ and $e \notin D$. Moreover, every strongly regular graph admitting a regular automorphism group can be obtained this way.
PDS and two weight codes.

**Theorem 28** Let $A = [a_1, \ldots, a_n] \in M_{s \times n}(\mathbb{F}_q)$ such that rank $A = s$ and $a_1, \ldots, a_n$ are pairwise linearly independent. Then $A$ generates an $(n, s)$ code with two nonzero weights $w_1$ and $w_2$ iff

$$D = \{ta_i : 1 \leq i \leq n, \ t \in \mathbb{F}_q^\times \}$$

is a PDS in $\mathbb{F}_q^s$ with parameters

$$\begin{align*}
v &= q^s, \\
k &= n(q - 1), \\
\lambda &= k^2 + 3k - q(k + 1)(w_1 + w_2) + q^2w_1w_2, \\
\mu &= k^2 + k - qk(w_1 + w_2) + q^2w_1w_2.
\end{align*}$$
Equation in group ring. Let $G$ be a finite group. Identify a subset $D \subset G$ with $\sum_{g \in D} g \in \mathbb{Z}[G]$. Define $D^{(-1)} = \sum_{y \in D} y^{-1}$. Then $D$ is a $(v = |G|, k = |D|, \lambda, \mu)$ PDS $\iff$

$$DD^{(-1)} = \mu G + (\lambda - \mu) D + \gamma e,$$

where

$$\gamma = \begin{cases} k - \mu & \text{if } e \notin D, \\ k - \lambda & \text{if } e \in D. \end{cases}$$

Call a PDS reversible if $D = D^{(-1)}$. All PDS with $\lambda \neq \mu$ are reversible [Ma94].

**Proposition 29** Let $G$ be a finite abelian group and $D \subset G$. Then $D$ is a reversible PDS iff $\exists \alpha, \beta \in \mathbb{R}$ such that

$$\chi(D) = \alpha \text{ or } \beta \quad \forall 1 \neq \chi \in \hat{G}. \quad (24)$$

When (24) is satisfied, the parameters of the PDS $D$ are

$$\begin{cases} v = |G|, \\ k = |D|, \\ \lambda = k + \alpha \beta + \delta (\alpha + \beta), \\ \mu = \lambda - (\alpha + \beta), \end{cases}$$

where

$$\delta = \begin{cases} 0 & \text{if } e \in D, \\ 1 & \text{if } e \notin D. \end{cases}$$
Proof of Example 26  Let $q = p^s$. Then every nontrivial character $\chi$ of $\mathbb{F}_q$ is of the form $\zeta_p^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)}$, $a \in \mathbb{F}_q^\times$. We have

$$\chi(D) = \frac{1}{2} \sum_{x \in \mathbb{F}_q^\times} \zeta_p^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)}$$

$$= \frac{1}{2} \left[ \sum_{x \in \mathbb{F}_q} \zeta_p^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax^2)} - 1 \right]$$

$$= \frac{1}{2} \left[ \pm q^\frac{1}{2} - 1 \right] \quad \text{(Gauss quadratic summ).}$$

So $\alpha = \frac{1}{2}(q^\frac{1}{2} - 1)$, $\beta = \frac{1}{2}(-q^\frac{1}{2} - 1)$, $\lambda = k + \alpha \beta + \alpha + \beta = \frac{1}{2}(q - 1) - \frac{1}{4}(q - 1) - 1 = \frac{1}{4}(q - 5)$, $\mu = \frac{1}{4}(q - 1)$. 

42
**Latin square type PDS.** Let $G$ be a finite abelian group with $|G| = n^2$. Let $D \subset G \setminus \{e\}$ be a reversible PDS such that

$$\chi(D) = -r \text{ or } -r + n \quad \forall 1 \neq \chi \in \hat{G},$$

where $r \in \mathbb{R}$. By (23),

$$DD = \mu G + (\lambda - \mu)D + (k - \mu)e$$

$$= (|D| - r(-r + n))G + (-2r + n)D + r(-r + n)e.$$  \hfill (25)

Counting the sum of coefficients at both sides of (25), we have

$$|D|^2 - |D|(n2 - 2r + n) + r(-r + n)(n^2 - 1) = 0,$$

which gives two solutions for $|D|:

$$|D| = r(n - 1) \text{ or } (n - r)(n + 1).$$

If $|D| = r(n - 1)$, $D$ is called a Latin square type PDS; if $|D| = (n - r)(n + 1)$, $D$ is called a negative Latin square type PDS.
Constructing Latin Square Type PDS by Latin Shells

**Latin shells.** Let $G ⊃ G_1 ⊃ G_2$ be finite abelian groups such that $|G| = |G_1||G_2|$ and let $r$ be a real number. A subset $D \subset G \setminus G_1$ is called a $(G, G_1, G_2; r)$-Latin shell if for each character $\chi$ of $G$,

$$\chi(D) =
\begin{cases}
  r|G|^\frac{1}{2}(1 - \frac{1}{|G_2|}), & \text{if } \chi \text{ is principal}, \\
  -r|G|^\frac{1}{2}, & \text{if } \chi \text{ is principal on } G_1 \text{ but not on } G, \\
  0, & \text{if } \chi \text{ is principal on } G_2 \text{ but not on } G_1, \\
  -r \text{ or } -r + |G|^\frac{1}{2}, & \text{if } \chi \text{ is not principal on } G_2.
\end{cases}$$

The group $G_2$ is called the thickness of the Latin shell $D$.

Note that when $G_1 = G_2$, a $(G, G_1, G_1; r)$-Latin shell is a Latin square type PDS with non principal character values $-r$ and $-r + |G|^\frac{1}{2}$. The following proposition shows that one can nest one Latin shell inside another to form a new Latin shell with greater thickness.
Proposition 30 Let $G \supset G_1 \supset G_2$ be finite abelian groups such that $|G| = |G_1||G_2|$ and let $D$ be a $(G, G_1, G_2; r)$-Latin shell. Let $G_1 \supset H_1 \supset H_2 \supset G_2$ be subgroups such that $|G_1||G_2| = |H_1||H_2|$ and let $E$ be a $(G_1/G_2, H_1/G_2, H_2/G_2; r/|G_2|)$-Latin shell. Let $\bar{E} \subset G_1 \setminus H_1$ be the pre image of $E$. Then $D \cup \bar{E}$ is a $(G, H_1, H_2; r)$-Latin shell.
Proposition 31 (Hou03) Let $R$ be a finite Frobenius local ring and $I$ a proper ideal of $R$. Let $r_R(I)$ be the right annihilator of $I$. Let $\sigma : r_R(I) \rightarrow \{0, 1\}$ be such that
\[
\sum_{x \in \text{soc}(R_R)} \sigma(a + x) = e \quad \text{for every } a \in r_R(I),
\]
where $e$ is any fixed integer with $0 \leq e \leq |\text{soc}(R_R)| = |R/\text{rad}(R)|$. Then
\[
D = \{(x, \bar{y}) \in [r_R(I) \times (R/I)] \setminus [r_R(I) \times (\text{rad}(R)/I)] : \sigma(y^{-1}x) = 1\}
\]
is an $(r_R(I) \times (R/I), r_R(I) \times (\text{rad}(R)/I), \text{soc}(R_R) \times \{0\}; e|\text{rad}(R)|/|I|)$-Latin shell where
\[
r_R(I) \times (R/I) \cong (R/I) \times (R/I)
\]
and
\[
[r_R(I) \times (\text{rad}(R)/I)] / [\text{soc}(R_R) \times \{0\}] \cong (\text{rad}(R)/I) \times (\text{rad}(R)/I)
\]
as abelian groups.
A Construction of Finite Frobenius Rings

The Latin shell in Proposition 31 construction applies to $R \times R$ whenever $R$ is a homomorphic image of a finite Frobenius local ring. So what kind of rings are homomorphic images of finite Frobenius local rings? We show that

- every finite ring is a homomorphic image of a finite Frobenius ring and

- every finite local ring is a homomorphic image of a finite Frobenius local ring.
Proposition 32 Let $R$ be a ring and $R^R_R$ an $(R,R)$-bimodule. Define $R \ltimes M = R \ltimes M$, and for each $(r_1,m_1), (r_2,m_2) \in R \ltimes M$, define

$$(r_1,m_1) + (r_2,m_2) = (r_1 + r_2, m_1 + m_2),$$

$$(r_1,m_1) \cdot (r_2,m_2) = (r_1r_2, r_1m_2 + m_1r_2).$$

Then $R \ltimes M$ is a ring with identity $(1,0)$. $R \times 0$ is a subring of $R \ltimes M$ and $R \times 0 \cong R$. $0 \times M$ is an ideal of $R \ltimes M$ and

$$R \longrightarrow (R \ltimes M)/(0 \times M)$$

$$r \longmapsto (r,0)$$

is a ring isomorphism.

The construction in Proposition 32 is known as the “trivial extension”. 
Let $R$ be a finite ring and let $R^\flat$ be the character group of $(R, +)$, i.e., $R^\flat = \text{Hom}(\mathbb{Z}R, \mathbb{Z}(\mathbb{Q}/\mathbb{Z}))$. Then $R^\flat$ is an $(R, R)$-bimodule: For each $\omega \in R^\flat$ and $a \in R$,

$$\omega a : R \to \mathbb{Q}/\mathbb{Z}$$

is defined by $(\omega a)(x) = \omega(ax)$ and

$$a\omega : R \to \mathbb{Q}/\mathbb{Z}$$

is defined by $(a\omega)(x) = \omega(xa)$.

**Theorem 33 (Hou-Nechaev 07)** Let $R$ be any finite ring. Then $R \rtimes R^\flat$ is a finite Frobenius ring. In fact

$$\chi : R \rtimes R^\flat \to \mathbb{Q}/\mathbb{Z}$$

$$(r, \omega) \mapsto \omega(1)$$

is a generating character of $R \rtimes R^\flat$.

**Proof.** Assume to the contrary that $\ker \chi$ contains a nonzero left ideal $I$ of $R \rtimes R^\flat$. First we claim that there is an element $(r, \omega) \in I$ such that $\omega \neq 0$. (Otherwise, choose $0 \neq (r, 0) \in I$. There is an $\omega \in R^\flat$ such that $\omega(r) \neq 0$. Then we have $(0, \omega) \cdot (r, 0) = (0, \omega r) \in I$, where $\omega r(1) = \omega(r) \neq 0$. Hence $\omega r \neq 0$.) Since $\omega \neq 0$, $\omega(s) \neq 0$ for some $s \in R$. Thus $(s, 0) \cdot (r, \omega) = (sr, s\omega) \in I$ but

$$\chi(sr, s\omega) = s\omega(1) = \omega(s) \neq 0,$$

which is a contradiction.

**Corollary 34** A finite ring is local if and only if it is a homomorphic image of a finite Frobenius local ring.
Proof. Let $R$ be a finite local ring. By Proposition 32 and Theorem 33, $R \cong (R \times R^y)/(0 \times R^y)$, where $R \times R^y$ is Frobenius. Since $(0 \times R^y)$ is a nilpotent ideal of $R \times R^y$, $R \times R^y$ is also local.

**Theorem 35** (i) Let $R$ be a finite local ring with residue field $R/{\text{rad}}(R) = \text{GF}(p^r)$. Then

$$(R, +) \cong \mathbb{Z}_{p^{n_1}}^{r_1} \times \mathbb{Z}_{p^{n_2}}^{r_2} \times \cdots \times \mathbb{Z}_{p^{n_k}}^{r_k} \tag{26}$$

where $n_1 > n_2 > \cdots > n_k \geq 1$, $r_i > 0$, and $r | r_i$ $(1 \leq i \leq k)$. Moreover,

$$(\text{rad}(R), +) \cong \mathbb{Z}_{p^{n_1}}^{r_1-r} \times \mathbb{Z}_{p^{n_1-1}}^{r} \times \mathbb{Z}_{p^{n_2}}^{r_2} \times \cdots \times \mathbb{Z}_{p^{n_k}}^{r_k} \tag{27}$$

(ii) For each prime $p$ and positive integers $n_i$, $r_i$ $(1 \leq i \leq k)$ and $r$ such that $n_1 > n_2 > \cdots > n_k \geq 1$ and $r | r_i$, there is a finite local ring $R$ such that $R/{\text{rad}}(R) = \text{GF}(p^r)$ and

$$(R, +) \cong \mathbb{Z}_{p^{n_1}}^{r_1} \times \mathbb{Z}_{p^{n_2}}^{r_2} \times \cdots \times \mathbb{Z}_{p^{n_k}}^{r_k} \tag{28}$$

$$(\text{rad}(R), +) \cong \mathbb{Z}_{p^{n_1}}^{r_1-r} \times \mathbb{Z}_{p^{n_1-1}}^{r} \times \mathbb{Z}_{p^{n_2}}^{r_2} \times \cdots \times \mathbb{Z}_{p^{n_k}}^{r_k} \tag{29}$$

**Theorem 36** Let $p$ be a prime and let $n_i$, $r_i$ $(1 \leq i \leq k)$ and $r$ be positive integers such that $n_1 > n_2 > \cdots > n_k$ and $r | r_i$. Let $G = \mathbb{Z}_{p^{n_1}}^{2r_1} \times \mathbb{Z}_{p^{n_2}}^{2r_2} \times \cdots \times \mathbb{Z}_{p^{n_k}}^{2r_k}$ and let $0 \leq e \leq p^r$. Then there exists a $(G, G_1, G_2; ep^{n_1r_1+\cdots+n_kr_k-r})$-Latin shell with $|G_2| = p^r$ and

$$G_1/G_2 \cong \mathbb{Z}_{p^{n_1}}^{2(r_1-r)} \times \mathbb{Z}_{p^{n_1-1}}^{2r} \times \mathbb{Z}_{p^{n_2}}^{2r_2} \times \cdots \times \mathbb{Z}_{p^{n_k}}^{2r_k}$$
Proof. By Theorem 35 (ii), there is a finite local ring $R$ such that $R / \text{rad}(R) = \text{GF}(p^r)$ and

$$(R, +) \cong \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$$

$$(\text{rad}(R), +) \cong \mathbb{Z}_{p^{n_1-r}} \times \mathbb{Z}_{p^{n_2-1}} \times \mathbb{Z}_{p^{n_3}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$$

By Corollary 34, there is a finite Frobenius local ring $T$ and an ideal $I \triangleleft T$ such that $R \cong T/I$. Note that $\text{rad}(T)/I \cong \text{rad}(R)$ and $|\text{rad}(T)|/|I| = |\text{rad}(R)| = p^{n_1 r_1 + \cdots + n_k r_k - r}$.

By Proposition 31, there is an $(R \times R, G_1, G_2; ep^{n_1 r_1 + \cdots + n_k r_k - r})$-Latin shell with $R \times R \cong G$, $|G_2| = |\text{soc}(R_R) \times \{0\}| = p^r$ and

$$G_1/G_2 \cong \text{rad}(R) \times \text{rad}(R) \cong \mathbb{Z}_{p^{n_1-r}} \times \mathbb{Z}_{p^{n_2-1}} \times \mathbb{Z}_{p^{n_3}} \times \cdots \times \mathbb{Z}_{p^{n_k}}.$$

**Corollary 37** In the notation of Theorem 36, there is a Latin square type PDS in $G$ with non principal character values $-e|G|^{1/2}/p^r$ and $|G|^{1/2} - e|G|^{1/2}/p^r$.

Proof. Simply use Theorem 36 and Proposition 30 repeatedly.
References


