6.962 Week 5

Topic: Irregular Repeat-Accumulate (IRA) Codes

Presenter: Stark Draper

Thanks to: F. R. Kschischang and
R. McEliece
for use of their slides.

Note: The slides available on-line from a subset of those presented in class. Some slides of F. Kschischang and R. McEliece were also used.

The “Final” Problem

For a given channel, find an ensemble of codes that:

(1) Has a linear-time encoding algorithm.

(2) Can be decoded reliably in linear time at rates arbitrarily close to channel capacity.

$\Rightarrow$ IRA codes satisfy (1), (2) on Binary Erasure Channel (BEC)!!

Outline

I. **IRA Codes & Factor Graphs**

II. BSC

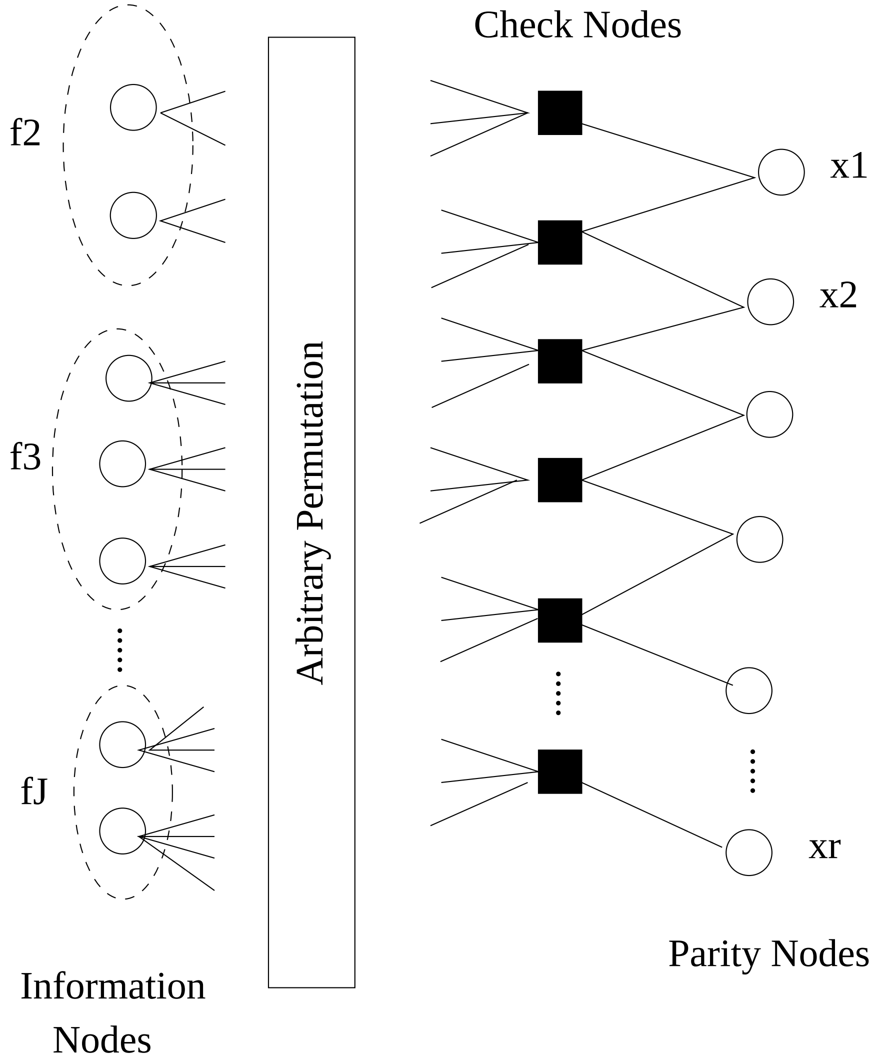
III. BEC

IV. Density Evolution

V. Computational Complexity

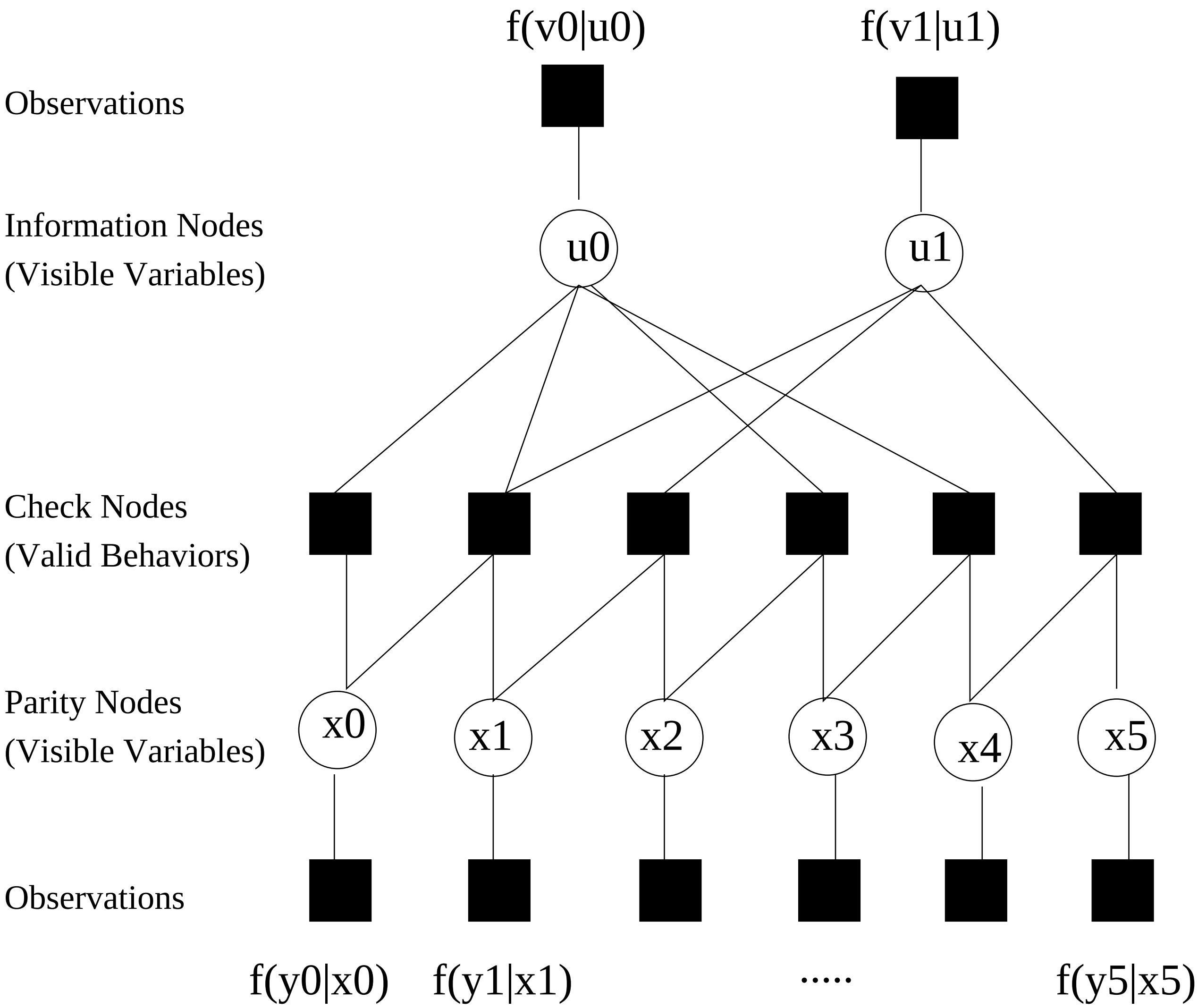
VI. IRA Code Performance

IRA codes vs. RA codes



RA codes	IRA codes
Info nodes const degree	Info nodes var degree
Chk nodes left degree 1	Chk nodes left degree a
Parity nodes degree 2	Parity nodes degree 2
Nonsystematic	Systematic

Factor Graph of IRA Code



Outline

I. IRA Codes & Factor Graphs

II. **BSC**

III. BEC

IV. Density Evolution

V. Computational Complexity

VI. IRA Code Performance

A Posteriori Probabilities

We transmit $(x_1, \ldots, x_N) = x_1^N$ over a memoryless channel.

We observe $(y_1, \ldots, y_N) = y_1^N$.

$$
\begin{aligned}
f(x_1^N | y_1^N) &= \frac{f(y_1^N | x_1^N) p(x_1^N)}{f(y_1^N)} \\
&\propto p(x_1^N) \prod_i f(y_i | x_i) \\
&= \underbrace{\frac{1}{|C|} \chi_C(x_1^N)}_{\text{Behavior}} \underbrace{\prod_i f(y_i | x_i)}_{\text{Probabilities}} .
\end{aligned}
$$

BSC: Probabilities

Joint Probabilities:

	$x=0$	$x=1$
$y=0$	$0.5(1-p)$	$0.5p$
$y=1$	$0.5*p$	$0.5(1-p)$

Initial probabilities to pass:

	$x=0$	$x=1$
$f(y=0\|x)$	$(1-p)$	p

	$x=0$	$x=1$
$f(y=1\|x)$	p	$(1-p)$

But, these change during decoding...

Binary Probability Gates 2

Can build multiple-input probability gates in terms of two-input gates, since:

$$\begin{aligned}\textbf{VAR}(x_1, x_2, \ldots, x_n) &= \textbf{VAR}(x_1, \textbf{VAR}(x_2, \ldots x_n)) \\ \textbf{CHK}(x_1, x_2, \ldots, x_n) &= \textbf{CHK}(x_1, \textbf{CHK}(x_2, \ldots x_n))\end{aligned}$$

Messages parameterize the density.

$$m = \log \left[\frac{p(x = 0; y)}{p(x = 1; y)} \right].$$

Multiplication is carried out on densities, not messages.

Outline

I. IRA Codes & Factor Graphs

II. BSC

III. **BEC**

IV. Density Evolution

V. Computational Complexity

VI. IRA Code Performance

BEC: Probabilities

Joint Probabilities:

	$x = 0$	$x = 1$
$y = 0$	$0.5(1 - p)$	0
$y = 1$	0	$0.5(1 - p)$
$y = e$	$0.5p$	$0.5p$

Initial probabilities to pass:

	$x = 0$	$x = 1$
$f(y = 0\|x)$	1	0

	$x = 0$	$x = 1$
$f(y = 1\|x)$	0	1

	$x = 0$	$x = 1$
$f(y = e\|x)$	0.5	0.5

BEC: Probabilities

Probabilities simplify greatly.

Summary:

1. $f(y|x) \sim B(1, 0)$ if $y = 0$.

2. $f(y|x) \sim B(0, 1)$ if $y = 1$.

3. $f(y|x) \sim B(0.5, 0.5)$ if $y = e$.

BEC: Messages Alphabet

1. $\log\left[\frac{f(y{=}0|x{=}0)}{f(y{=}0|x{=}1)}\right] = \log[1/0] = +\infty.$

$\Rightarrow m = m_0.$

2. $\log\left[\frac{f(y{=}1|x{=}0)}{f(y{=}1|x{=}1)}\right] = \log[0/1] = -\infty.$

$\Rightarrow m = m_1.$

3. $\log\left[\frac{f(y{=}e|x{=}0)}{f(y{=}e|x{=}1)}\right] = \log[0.5/0.5] = 0.$

$\Rightarrow m = m_e.$

Message alphabet doesn't change during decoding!!!

BEC: Message Alphabet

Message alphabet reduces to three letters:

1. $m = m_0$ if $\log \left[\frac{f(y{=}0|x{=}0)}{f(y{=}0|x{=}1)} \right] = +\infty$

2. $m = m_1$ if $\log \left[\frac{f(y{=}1|x{=}0)}{f(y{=}1|x{=}1)} \right] = -\infty$.

3. $m = m_e$ if $\log \left[\frac{f(y{=}e|x{=}0)}{f(y{=}e|x{=}1)} \right] = 0$.

BEC: Factor-Graphs rules

Node output rules simplify:

- A variable node outgoing message is m_0 (m_1) **if any** incoming messages is m_0 (m_1) (i.e. not all incoming messages are erasures, m_e). Having one incoming message m_0 and another m_1 is impossible on the BEC.

- A check node outgoing message is m_0 (m_1) **only if all** incoming messages are non-erasures and sum to m_0 (m_1). (A single erasure incoming message completely randomizes output of parity check.)

- If neither of the above holds, the outgoing message is m_e.

Outline

I. IRA Codes & Factor Graphs

II. BSC

III. BEC

IV. **Density Evolution**

V. Computational Complexity

VI. IRA Code Performance

Fixed-Point Analysis

1. Assume decoding has converged.

2. Calculate ensemble-average erasure probabilities (x_0, x_1, x_2, x_3)

3. Eliminate x_1, x_2, x_3 to leave an equation parameterized by x_0.

4. Show $x_0 \notin (0, 1]$.

$\Rightarrow$ $x_0 = \text{Pr(erasure on info bit)} \to 0$.

Fixed-point Pr(erasure) Calculation

Condition on the degree of the node:

$$
\begin{aligned}
x_1 &= \text{Pr}(m = m_e, \text{chk} \rightarrow \text{parity}) \\
&= \sum_{i=1}^{D_{\text{max}}} \text{Pr}(m_e, \text{chk node deg i}) \\
&= \sum_{i=1}^{D_{\text{max}}} \left[1 - \text{Pr}(\overline{m_e} | \text{deg i})\right] \text{Pr}(\text{deg i}) \\
&= \sum_{i=1}^{D_{\text{max}}} \left[1 - (1 - x_2) \prod_{j=1}^{i} (1 - x_0)\right] \text{Pr}(\text{deg i}) \\
&= 1 - (1 - x_2) \sum_i (1 - x_0)^i \left[\frac{\rho_i}{i} \frac{1}{\sum(\rho_j / j)}\right] \\
&= 1 - (1 - x_2) R(1 - x_0).
\end{aligned}
$$

And similarly for x_0, x_2, x_3.

Summary

$x_i^{(L)}$ is the value of x_i on the Lth iteration.

$$\begin{aligned}
x_1[L] &= 1-(1-x_2[L])R(1-x_0[L]), \\
x_2[L] &= px_1[L], \\
x_3[L] &= 1-(1-x_2[L])^2\rho(1-x_0), \\
x_0[L+1] &= p\lambda(x_3[L]).
\end{aligned}$$

Which becomes

$$x_0[L+1] = p\lambda\left(1-\left[\frac{1-p}{1-pR(1-x_0[L])}\right]^2\rho(1-x_0[L])\right)$$

Show must converge to a point $x_0 \notin (0,1]$.

Outline

I. IRA Codes & Factor Graphs

II. BSC

III. BEC

IV. Density Evolution

V. **Computational Complexity**

VI. IRA Code Performance

Outline

I. IRA Codes & Factor Graphs

II. BSC

III. BEC

IV. Density Evolution

V. Computational Complexity

VI. **IRA Code Performance**