# Entropy Approximation for FCSRs

Andrea Röck

Limoges, 13th February 2007

INRIA

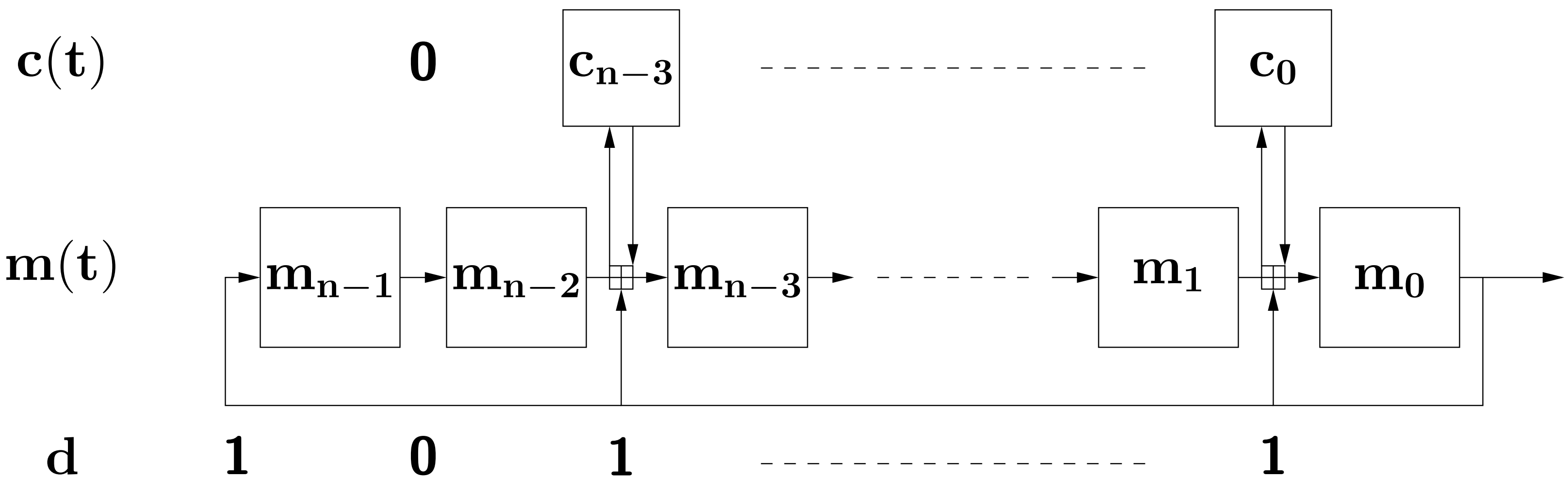
# Outline

- FCSR
- Entropy after one Feedback
- Final Entropy
  - Method
  - Algorithm
  - Approximations
- Results

# Part 1

# FCSR

# Feedback with Carry Shift Register




- $m(t)$ main register
- $c(t)$ carry register
- $d$ determines feedback, $2^{n-1} \leq d < 2^n$

# Notations

- $n$ length of main register
- $m = \sum_{i=0}^{n-1} m_i \, 2^i$
- $d^* = d - 2^{n-1}$
- $I_d = \{i | 0 \leq i \leq n-2 \text{ and } d^*_i = 1\}$
- $\ell = HammingWeight(d^*)$
- $c = \sum_{i \in I_d} c_i \, 2^i$
- $(m(t), c(t))$ state after $t$ iterations

# State Update Function

- $i = n - 1$

$$m_{n-1}(t+1) = m_0(t)$$

- $0 \le i < n-1$ and $i \in I_d$

$$\begin{array}{ccccccccc} \langle & c_i, & m_i & \rangle(t+1) & = & m_{i+1}(t) & + & c_i(t) & + & m_0(t) \\ & 1 & 0 & & = & 1 & + & 0 & + & 1 \end{array}$$

- $0 \le i < n-1$ and $i \notin I_d$

$$m_i(t+1) = m_{i+1}(t)$$

# [Klapper, Goresky 94]

- Let
  - $q := 1 - 2\,d$
  - $p := m + 2c$

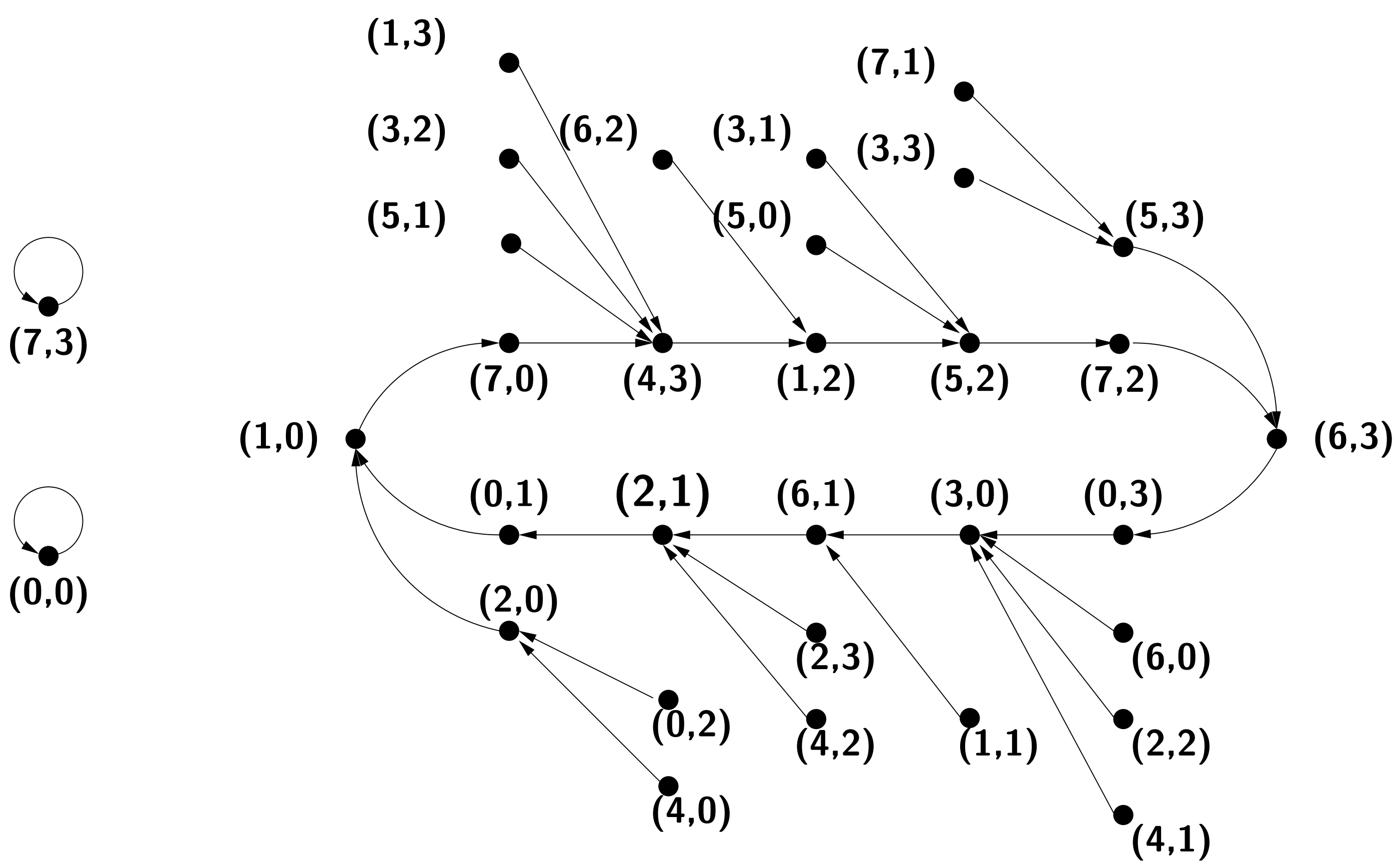
It holds that

- $0 \leq p \leq |q|$
- Output of FCSR is $2$-adic expansion of $\frac{p}{q}$
- Two fixed points $(0, 0)$ and $(2^n - 1, d^*)$

# e.g. [Koblitz 97]

▷ If $q$ is odd, $p$ and $q$ are coprime and the order of $2$ modulo $q$ is $|q| - 1$ then the FCSR has the maximal period of $|q| - 1$. In this case we say the FCSR is *optimal*.

# Functional Graph



# Entropy of State at time $t$

- $p_{(m,c)}(t)$ probability of the state being $(m, c)$ at time $t$.
- $(m(0), c(0))$ is uniformly distributed.
- $p_{(m,c)}(t)$ is well defined due to initial distribution.
- Entropy:

$$H(t) := \sum_{(m,c)} p_{(m,c)}(t) \log_2 \frac{1}{p_{(m,c)}(t)}$$

# Part 2

## Entropy after one Feedback

# Entropy after one Feedback

- **Initial entropy:** $n + \ell$
- **Question:**
  Entropy loss after one feedback?
- **Method:**
  Count the number of $(m(0), c(0))$'s which produce the same $(m(1), c(1))$.

# Fix $(\mathbf{m(1)}, \mathbf{c(1)})$

- From $m_{n-1}(t+1) = m_0(t)$: $m_0(0)$
- $i \notin I_d$: From $m_i(t+1) = m_{i+1}(t)$: $m_{i+1}(0)$
- $i \in I_d$: From

$$\langle c_i, m_i \rangle (t+1) = m_{i+1}(t) + c_i(t) + m_0(t)$$

same $(m_i(1), c_i(1))$ with

$$(m_{i+1}(0), c_i(0)) = (0,1) \text{ or } (1,0)$$

# Method (1)

- $j$: number of $i \in I_d$ where $m_i(1) \neq m_0(0)$ and thus $m_{i+1}(0) \neq c_i(0)$.
- $(m(1), c(1))$ can be produced by $2^j$ different $(m(0), c(0))$'s.
- There are $2^{n-j}\binom{\ell}{j}$ such $(m(1), c(1))$'s

# Method (2)

- Entropy after one iteration:

$$\sum_{j=0}^{\ell} 2^{n-j} \binom{\ell}{j} \frac{2^j}{2^{n+\ell}} \log_2 \frac{2^{n+\ell}}{2^j} = n + \frac{\ell}{2}$$

# Part 3

# Final Entropy

# Final Entropy

- **Goal:** Entropy when we reached the cycle
- **Idea:** How many $(m, c)$'s create the same $p = m + 2c$.

# Final Entropy

## Method

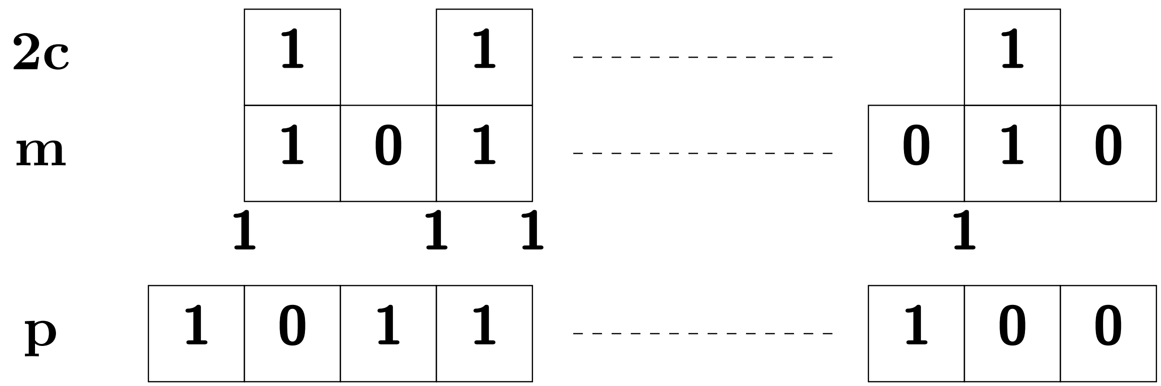
# [Arnault, Berger, Minier - SASC 07] (1)

- **Definition:**
  Two states $(m, c)$ and $(m', c')$ are said equivalent if $m + 2c = m' + 2c' = p$.
- **Proposition:**
  Two non-invariant states of a FCSR automaton with optimal period are equivalent if and only if they converge to the same state of the main cycle in the same number of steps.

# [Arnault, Berger, Minier - SASC 07] (2)

- **Theorem:**
  The length of the tail of the graph of an optimal FCSR automaton is at most $n + 3$.

# Method (1)




Bitwise addition with carry

# Method (2)

- We group $p$ with similar binary representation into sets $B_i$.
- Each time we calculate
  - $G(i) = \#\{(m,c) : p = m + 2c\}$ for $p \in B_i$
  - $|B_i|$
  - fraction of entropy

$$|B_i| \, \frac{G(i)}{2^{n+\ell}} \log_2 \left( \frac{2^{n+\ell}}{G(i)} \right)$$

# Final Entropy

## Algorithm

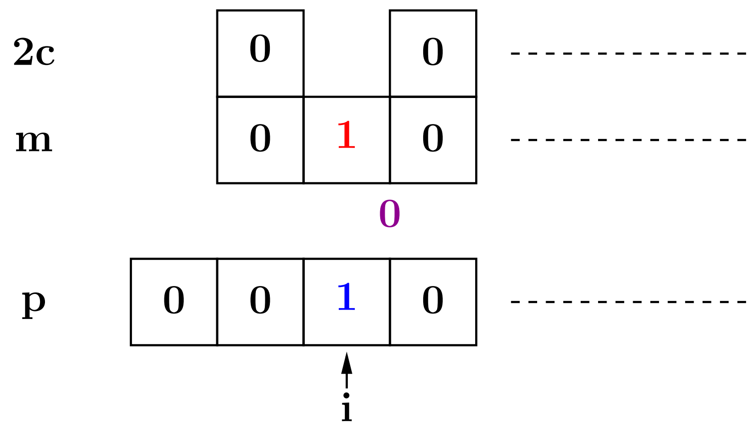
# Case $\mathbf{p < 2^n}$

- $i = \lfloor \log_2(p) \rfloor$
- $\ell' = \#\{j \in I_d | j \leq i\}$

- Two cases:
  - $d_{i-1} = 0$
  - $d_{i-1} = 1$

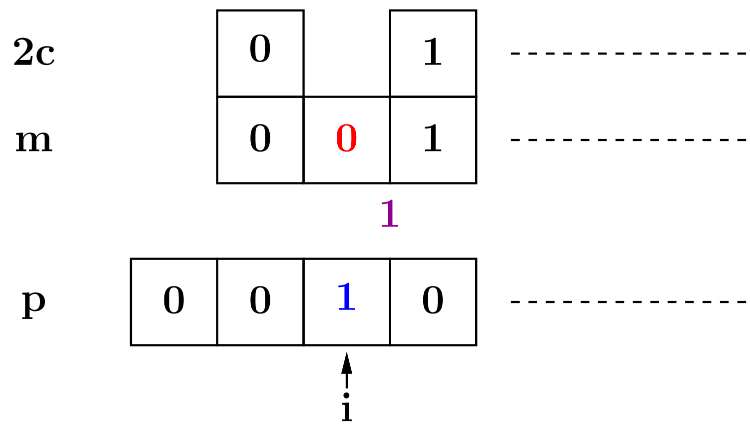
# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 0}$ (1)

- Not important if we have a carry at $i-1$
- $2$ possibilities at each feedback position



# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 0}$ (1)

- Not important if we have a carry at $i-1$
- $2$ possibilities at each feedback position



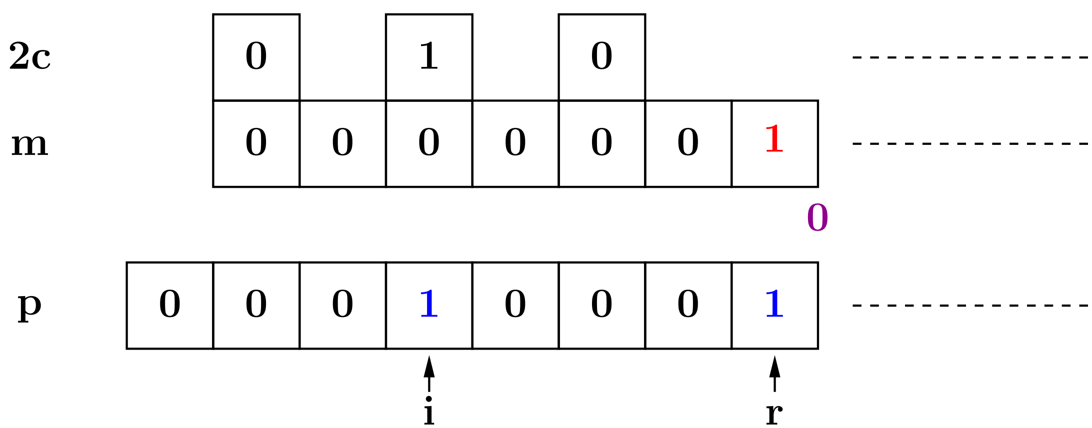
# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 0}$ (2)

- $2^{\ell'}$ possible $(m,c)'s$
- $2^i$ such $p$'s
- Fraction of entropy:

$$2^i 2^{\ell' - n - \ell}(n + \ell - \ell')$$

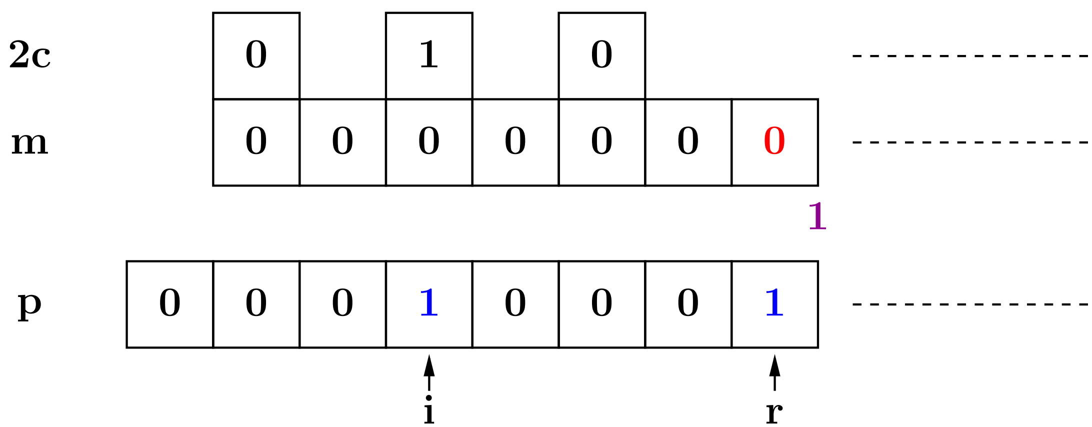
# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (1)

- $r(p) = \max\{j < i | d_{j-1} = 0, p_j = 1\}$
- No carry can be forwarded over $r$
- Possible range: $-1 \leq r < i$



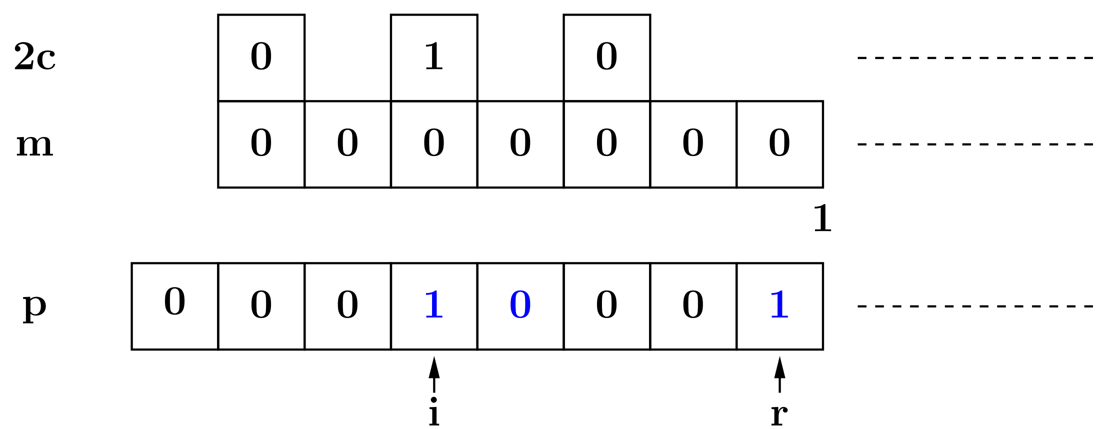
# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (1)

- $r(p) = \max\{j < i | d_{j-1} = 0, p_j = 1\}$
- No carry can be forwarded over $r$
- Possible range: $-1 \leq r < i$



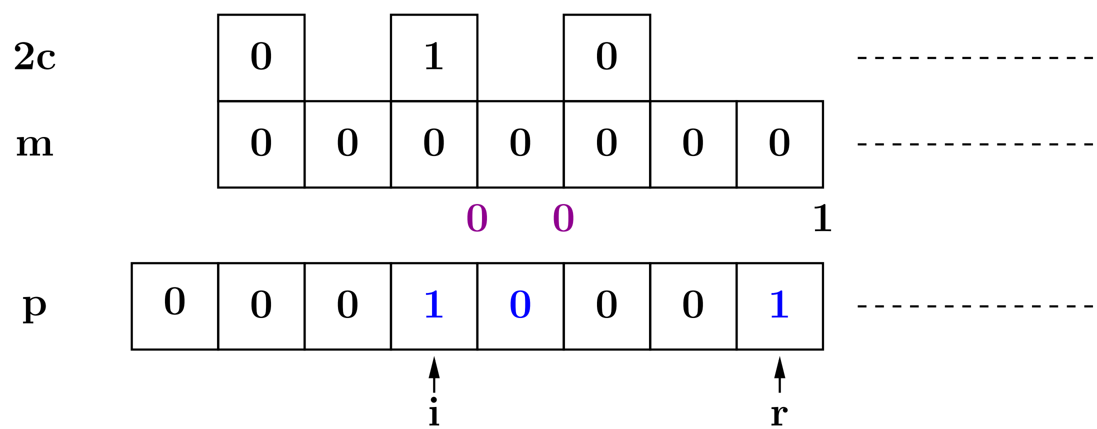
# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (2)

- For $i > j > r$ with $d_{j-1} = 0$:
  - $p_j = 0$ (definition of $r(p)$)
  - carry is forwarded



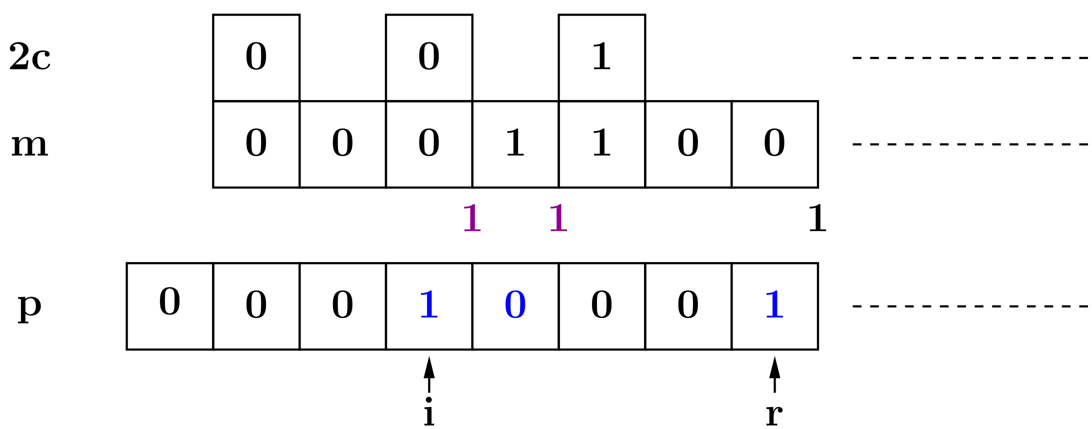
# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (2)

- For $i > j > r$ with $d_{j-1} = 0$:
  - $p_j = 0$ (definition of $r(p)$)
  - carry is forwarded



# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (2)

- For $i > j > r$ with $d_{j-1} = 0$:
  - $p_j = 0$ (definition of $r(p)$)
  - carry is forwarded



# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (3)

- $\ell'' = \#\{j \in I_d | j < r\}$
- $I_{d'}(r, i) = \{j | r < j < i$ and $d_{j-1} = 1\}$
- $p'$ and $(m', c')$:
  $p$ and $(m, c)$ reduced on $I_{d'}(r, i)$
- $x(p')$:
  number of possibilities for $m'$ and $c'$ to generate $p'$ but *with* a carry at position $i - 1$.

# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (4)

- ▷ For all $0 \leq x \leq 2^{\ell' - \ell'' - 1} - 1$ there exists exactly one $p'$ with $x(p') = x$.
- ▷ carry at $i - 1$: $(m_i, c_{i-1}) = (0, 0)$
- ▷ no carry at $i - 1$: $(m_i, c_{i-1}) = (1, 0)$ or $(0, 1)$
- ▶ possible $(m', c')$ to create $1p'$

$$x(p') + 2(2^{\ell' - \ell'' - 1} - x(p')) = 2^{\ell' - \ell''} - x(p')$$

- ▶ $2^r$ $p$s for each $p'$

# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (4)

- Fix $i$ and $r$
- $y\ 2^{\ell''}$ possible $(m, c)'s$, for all $2^{\ell'-\ell''-1} + 1 \leq y \leq 2^{\ell'-\ell''}$
- $2^r\ 2^{\ell'-\ell''-1}$ such $p$'s

# $\mathbf{p < 2^n}$ and $\mathbf{d_{i-1} = 1}$ (5)

- Fraction of entropy:

$$2^{r+\ell'-2-n-\ell} \quad \left(3\ 2^{\ell'-\ell''-1} + 1\right)(n + \ell - \ell'')$$

$$- \quad 2^{r+\ell''-n-\ell} \quad \sum_{y=2^{\ell'-\ell''-1}+1}^{2^{\ell'-\ell''}} y \log_2(y)$$

- For $r = -1$ we replace $2^r$ by $1$.

## $\mathbf{2^n \leq p < |q|}$ (1)

- Need carry at position $n-1$
- $r(p)$, $\ell''$, $I_{d'}$, $p'$, $(m', c')$, and $x(p')$ defined as above
- $r(p) < \log_2(d^*) + 1$, otherwise $p > |q|$.
- Possible range: $-1 \leq r < \log_2(d^*) + 1$
- For all $1 \leq x \leq 2^{\ell - \ell''} - 1$ there exists exactly one $p'$ with $x(p') = x$. (Exclude $x(p') = 0$ since there is no possibility for a carry.)
- $2^r$ $p$s for each $p'$

## $\mathbf{2^n \le p < |q|}$ (2)

- Fix $r$
- $x\,2^{\ell''}$ possible $(m,c)'s$, for each $1 \le x \le 2^{\ell-\ell''} - 1$.
- $2^r \left(2^{\ell-\ell''} - 1\right)$ such $p$'s

# $\mathbf{2^n \leq p < |q|}$ **(3)**

- Fraction of entropy:

$$
\begin{aligned}
& 2^r\, 2^{-n-1} \quad (2^{\ell-\ell''}-1)\,(n+\ell-\ell'') \\
- \;\; & 2^r\, 2^{\ell''-n-\ell} \quad \sum_{x=1}^{2^{\ell-\ell''}-1} x \log_2(x)
\end{aligned}
$$

- For $r=-1$ we replace $2^r$ by $1$.

# Final Entropy

## Approximations

# Problem

- Complexity of Algorithm $O\left(n^2\right)$ if we know value of the sums.
- Calculation of

$$\sum_{x=1}^{2^k-1} x\log_2(x) \text{ and } \sum_{x=2^{k-1}+1}^{2^k} x\log_2(x)$$

impractical for large $k$

# Upper / Lower Bound

As we know the indefinite integral of $x \mapsto x\log_2(x)$ we can use:

$$\int_{2^{k-1}}^{2^k} x\log_2(x)dx < \sum_{x=2^{k-1}+1}^{2^k} x\log_2 x < \int_{2^{k-1}+1}^{2^k+1} x\log_2(x)dx$$

$$\int_{1}^{2^k} x\log_2(x)dx < \sum_{x=1}^{2^k} x\log_2 x < \int_{2}^{2^k+1} x\log_2(x)dx$$

# Better Approximation (1)

- **Idea:**

$$\int_x^{x+1} y\log_2(y) \approx \frac{1}{2}\Big(x\log_2(x) + (x+1)\log_2(x+1)\Big)$$

- Good approximation for large $k$.

# Better Approximation (2)

- Get

$$\sum_{y=2^{k-1}+1}^{2^k} y \log_2 y \;=\; 2^{2k-3}\left(3k+1-\frac{3}{2\ln(2)}\right) +2^{k-2}(k+1)+O(1)$$

$$\sum_{y=1}^{2^k-1} y \log_2 y \;=\; 2^{2k-1}\left(k-\frac{1}{2\ln(2)}\right) - k2^{k-1} + O(1)$$

# Part 4

# Results

# Results

| $n$ | $d$ | $\ell$ | entropy | $\log_2(\lvert q\rvert - 1)$ |
|---|---|---|---|---|
| $16$ | $O\text{x}A54E$ | $7$ | $16.2728$ | $16.3689$ |
| $24$ | $O\text{x}A59B4E$ | $12$ | $24.2733$ | $24.3716$ |

| $n$ | $d$ | lower bound | upper bound | approx |
|---|---|---|---|---|
| $16$ | $O\text{x}A54E$ | $16.1005$ | $16.4173$ | $16.2728$ |
| $24$ | $O\text{x}A59B4E$ | $24.1063$ | $24.4131$ | $24.2733$ |

- For $k < 5$, I used the real value of the sums in the approximation.