List decoding of Reed-Muller codes with linear complexity up to the Johnson bound

Rafaël Fourquet

Univ. Paris 8, France

ACCT 2012

Binary Reed-Muller Codes

- Boolean function in m-variables:

$$\mathcal{B}_m = \{f : \mathbb{F}_2^m \longmapsto \mathbb{F}_2\}$$

- Truth table of f: the list of its values (an order in $\mathbb{F}_2^m$ is fixed)

$$f = (f(0), f(1), \ldots, f(2^m - 1) \in \mathbb{F}_2^{2^m}$$

- Algebraic Normal Form:

$$\mathcal{B}_m \simeq \mathbb{F}_2[x_1, \ldots, x_m]/(x_i^2 - x_i)$$

- Reed-Muller code of order r in m variables:

$$\mathrm{RM}(r, m) = \{\text{polynomials of degrees} \leq r\} \subset \mathbb{F}_2^{2^m}$$

$\longrightarrow$ Linear code of length $n = 2^m$, dimension $\sum_{i=0}^{r} \binom{m}{i}$ and minimal distance 2^{m-r}.

List decoding

Let $f \in \mathcal{B}_m$ be a received vector, $\varepsilon \in]0,1]$. A deterministic list decoding algorithm for the $\mathrm{RM}(r,m)$ code outputs the list

$$L_\varepsilon(f) = \left\{ q \in \mathrm{RM}(r,m) \ : \ \mathrm{d}(f,q) \leq 2^{m-1}(1-\varepsilon) \right\}.$$

where $\mathrm{d}(f,q)$ is the Hamming distance between f and q.

Definitions

Description of the algorithm

Experimental results

Sums Algorithm

- Sums algorithm in $\mathrm{RM}(1, m)$ (Kabatiansky-Tavernier, ACCT'04)
  - Goldreich-Levin algorithm: coefficients of the solutions are constructed one by one
  - Fast Fourier Transform (FFT): efficient use of the recursive structure of $\mathrm{RM}(1, m)$
- proposed algorithm: extension of the sums algorithm to any order

Representation of a Boolean function

- coefficients of a Boolean function $q \in \mathrm{RM}(r, m)$ of degree r:

$$\begin{aligned} q(x_1, \dots, x_m) &= x_1 T_1(x_2, \dots, x_m) \\ &+ x_2 T_2(x_3, \dots, x_m) \\ &+ \cdots \\ &+ x_{m-1} T_{m-1}(x_m) \\ &+ x_m T_m \end{aligned}$$

  with $T_i(x_{i+1}, \dots, x_m) \in \mathrm{RM}(r-1, m-i)$
- Definition: the i-prefix q^i of q:

$$q^i = x_1 T_1(x_2, \dots, x_m) + \cdots + x_i T_i(x_{i+1}, \dots, x_m) \in \mathrm{RM}(r, m)$$

- At the i-th step of the algorithm, determine a list L^i of potential i-prefix of the solutions

Representation of a Boolean function

Example:

$$\begin{aligned} q &= x_1x_3 + x_2x_3 + x_2x_4 + x_3x_4 \\ &= x_1 \underbrace{(x_3)}_{T_1} + x_2 \underbrace{(x_3 + x_4)}_{T_2} + x_3 \underbrace{(x_4)}_{T_3} \end{aligned}$$

$$q^1 = x_1(x_3)$$

$$q^2 = x_1(x_3) + x_2(x_3 + x_4)$$

$$q^2 = x_1(x_3) + x_2(x_3 + x_4) + x_3(x_4)$$

The sums metric

$$q \in L_\varepsilon(f) \iff \sum_{x\in\mathbb{F}_2^m} (-1)^{f(x)+q(x)} = n - 2\mathrm{d}(f,q) \geq n\varepsilon \qquad (n = 2^m)$$

Lemma

Let $1 \leq i \leq m$. For all fixed $\alpha \in \mathbb{F}_2^{m-i}$, we have

$$q^m(x,\alpha) = q^i(x,\alpha) + q(0,\ldots,0,\alpha)$$

Hence:

$$\sum_{x\in\mathbb{F}_2^m} (-1)^{f(x)+q^m(x)} = \sum_{\alpha\in\mathbb{F}_2^{m-i}} (-1)^{q(0,\ldots,0,\alpha)} \sum_{x\in\mathbb{F}_2^i} (-1)^{f(x,\alpha)+q^i(x,\alpha)}$$

$$q \in L_\varepsilon(f) \Rightarrow \Gamma^i(q) := \sum_{\alpha\in\mathbb{F}_2^{m-i}} \left| \sum_{x\in\mathbb{F}_2^i} (-1)^{f(x,\alpha)+q^i(x,\alpha)} \right| \geq n\varepsilon$$

$$\boxed{L^i = \left\{ q^i \ : \ \Gamma^i(q^i) \geq n\varepsilon \right\}}$$

Computing the criterion Γ^i

$F_i(\alpha) := \sum_{x \in \mathbb{F}_2^i} (-1)^{f(x,\alpha)+q^i(x,\alpha)}$
$\Gamma^i(q^i) = \sum_{\alpha \in \mathbb{F}_2^{m-i}} |F_i(\alpha)|$
Let $q^i = q^{i-1} + x_i T_i$. For $x \in \mathbb{F}_2^{i-1}, \alpha \in \mathbb{F}_2^{m-i}$:

$$q^i(x,0,\alpha) = q^{i-1}(x,0,\alpha)$$
$$q^i(x,1,\alpha) = q^{i-1}(x,1,\alpha) + T_i(\alpha)$$

Hence:

$$F_i(\alpha) = F_{i-1}((0,\alpha)) + (-1)^{T_i(\alpha)} F_{i-1}((1,\alpha))$$

$\longrightarrow$ F_{i-1} was computed at the previous step.

A recursive algorithm

Problem: given $q^{i-1} \in L^{i-1}$, how to compute the list $T(q^{i-1}) := \{ T_i \in \mathrm{RM}(r-1, m-i) \ : \ q^{i-1} + x_i T_i \in L^i \}$ of successors of q^{i-1}?
$\longrightarrow$ it is a list decoding problem in $\mathrm{RM}(r-1, m-i)$!

Algorithm: given $q^{i-1} \in L^{i-1}$ and F_{i-1}:

- compute $T(q^{i-1})$ using F_{i-1}
- $\forall T_i \in T(q^{i-1})$:
  - $q^i \leftarrow q^{i-1} + x_i T_i$
  - compute F_i from F_{i-1} and T_i
  - apply recursively the algorithm to q^i and F_i

Computing $T(q^{i-1})$

Let

$$V(0,\alpha) = |F_{i-1}((0,\alpha)) + F_{i-1}((1,\alpha))|$$
$$V(1,\alpha) = |F_{i-1}((0,\alpha)) - F_{i-1}((1,\alpha))|$$

Then we have by definition:

$$\Gamma^i(q^{i-1} + x_i T_i) = \sum_{\alpha\in\mathbb{F}_2^{m-i}} |F_i(\alpha)| = \sum_{\alpha\in\mathbb{F}_2^{m-i}} V(T_i(\alpha),\alpha)$$

Let

$$S(\alpha) = (V(0,\alpha) + V(1,\alpha))/2$$
$$D(\alpha) = (V(0,\alpha) - V(1,\alpha))/2$$

Then:

$$V(T_i(\alpha),\alpha) = S(\alpha) + (-1)^{T_i(\alpha)} D(\alpha).$$

We deduce:

$$T_i \in T(q^{i-1}) \Leftrightarrow \sum_{\alpha} (-1)^{T_i(\alpha)} D(\alpha) \geq n\varepsilon - \sum_{\alpha} S(\alpha)$$

Size of the lists and complexity

Theorem (Johnson bound)

If $\varepsilon > \sqrt{1 - 2^{1-r}}$, *then*

$$|L_\varepsilon(f)| \leq \frac{2^{1-r}}{\varepsilon^2 - 1 + 2^{1-r}}$$

Lemma

The Johnson bound applies to the intermediate lists L^i.

Theorem

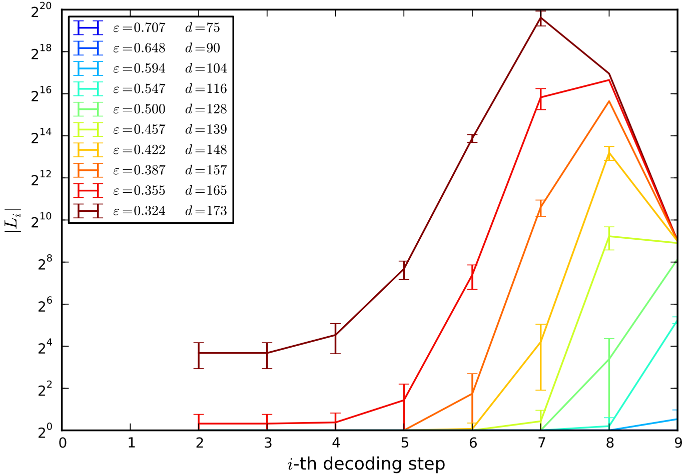
For fixed r *and* $\varepsilon > \sqrt{1 - 2^{1-r}}$, *the algorithm has linear complexity.*

Proof.

$$\theta(r, m) = \sum_{i=1}^{m} \left| L^{i-1} \right| \times (\underbrace{\theta(r-1, m-i)}_{\text{computing } T(q^{i-1})} + \underbrace{O(2^{m-i+1})}_{\text{computing } F_{i-1}})$$

□

Size of the lists in the BSC for $\mathrm{RM}(2,9)$



Non-linearity profile

Non-linearity of order r of a Boolean function f:

$$nl_r(f) = \min_{q \in \mathrm{RM}(r,m)} \mathrm{d}(f, q)$$

Non-linearity profile of the "inverse" function $\mathrm{tr}(x^{-1}) : \mathbb{F}_{2^8} \to \mathbb{F}_2$

r	1	2	3	4	5	6	7	8
nl_r	112	82	48	22	8	2	0	0
$\dim \mathrm{RM}(r, 8)$	9	37	93	163	219	247	255	256

Thank you