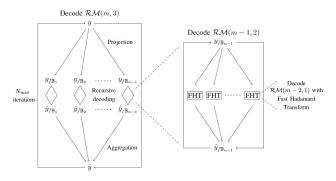
An Analysis of Recursive Projection-Aggregation Decoding of Reed-Muller Codes

Arvind Rameshwar
IIT Madras

CodelT: CNI Workshop on Codes, Sequences and Information Theory Happy 70th, Prof. Vijay Kumar!

What is this talk about?

Consider the family of binary Reed-Muller (RM) codes.



Source: [Ye-Abbe (2020)]

We show that the Recursive Projection-Aggregation (RPA) decoder of [Ye-Abbe (2020)] achieves vanishing error probabilities over the BSC for RM codes of low rate.

Brief background: RM codes

- Fix $m \ge 1$ and consider the points (x_1, \ldots, x_m) of the Boolean hypercube $\{0, 1\}^m$.
- ▶ Define $x_S := \prod_{i \in S} x_i$, where $S \subseteq [m]$.
- ▶ Pick a multilinear polynomial $f = \sum_{S \in \mathcal{S}} x_S$, where $S \subseteq \mathcal{P}([m])$, with

$$\deg(f) = \max_{S \in \mathcal{S}} |S| \le r.$$

Evaluate f at all points in $\{0,1\}^m$ in the (lexicographic) order:

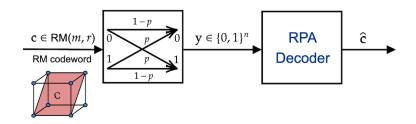
$$000\dots00 \rightarrow 000\dots01 \rightarrow 000\dots10 \rightarrow \dots \rightarrow 111\dots11$$
,

and call the resultant vector Eval(f). Here, blocklength $n = 2^m$.

- ▶ The code RM(m, r) consists of all Eval(f), where f is as above.
- ▶ $\dim(RM(m,r)) = \#\{x_S : \deg(x_S) = |S| \le r\} = \sum_{i=0}^r {m \choose i} = {m \choose \le r}.$

Problem setup

Consider the transmission of an RM codeword across a binary symmetric channel (BSC).



Q: How large can the rate be for $\Pr[\widehat{\mathbf{c}} \neq \mathbf{c}] \xrightarrow{N \to \infty} 0$?

TL;DL: The parameter r can grow \approx logarithmically in m

Placing things in context

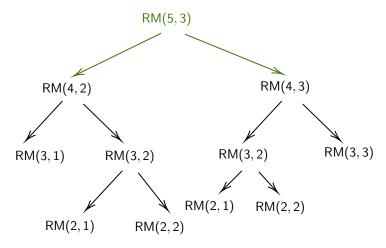
- ▶ [Reed (1954)] provided a decoder capable of correcting $<\frac{d_{\min}}{2}$ adversarial errors.
- For first-order (r = 1) RM codes, [Green (1966)] and [Be'ery-Snyders (1986)] described efficient ML decoding, via the Fast Hadamard Transform (FHT).
- ► For second-order RM codes, see [Sidel'nikov-Pershakov (1992)] and [Sakkour (2005)] for decoders that work well at moderate blocklengths.
- ▶ Provably good error guarantees over the BSC for constant r obtained via [Dumer (2004, 2006), Dumer-Shabunov (2006)]
- ► More recently, data-driven decoding methods have been explored [Jamali et al. (2023)]

Placing things in context

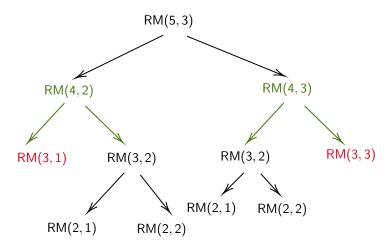
- ▶ [Reed (1954)] provided a decoder capable of correcting $<\frac{d_{\min}}{2}$ adversarial errors.
- For first-order (r = 1) RM codes, [Green (1966)] and [Be'ery-Snyders (1986)] described efficient ML decoding, via the Fast Hadamard Transform (FHT).
- ► For second-order RM codes, see [Sidel'nikov-Pershakov (1992)] and [Sakkour (2005)] for decoders that work well at moderate blocklengths.
- ▶ Provably good error guarantees over the BSC for constant r obtained via [Dumer (2004, 2006), Dumer-Shabunov (2006)]
- ► More recently, data-driven decoding methods have been explored [Jamali et al. (2023)]

Simulations [Ye-Abbe (2020), Li et al. (2021), Fathollahi et al. (2021)] demonstrate good performance of the RPA decoder for "low" r values.

Via the Plotkin decomposition, \underline{R} ecursive(ly) \underline{P} roject using all one-dimensional subspaces

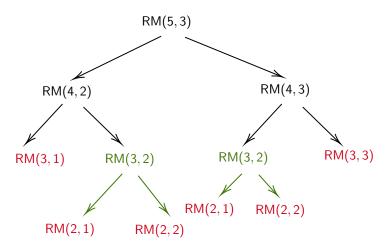


Via the Plotkin decomposition, \underline{R} ecursive(ly) \underline{P} roject using all one-dimensional subspaces



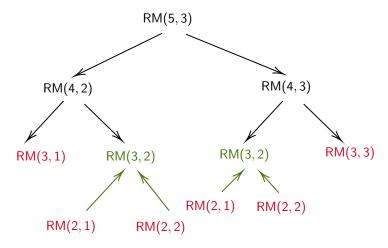
ML decode at red codes

Via the Plotkin decomposition, \underline{R} ecursive(ly) \underline{P} roject using all one-dimensional subspaces

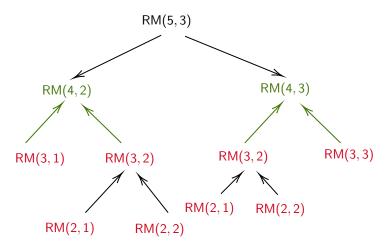


ML decode at red codes

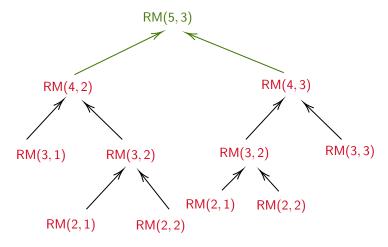
Via the Plotkin decomposition, \underline{R} ecursive(ly) \underline{P} roject using all one-dimensional subspaces and \underline{A} ggregate decoded estimates



Via the Plotkin decomposition, \underline{R} ecursive(ly) \underline{P} roject using all one-dimensional subspaces and \underline{A} ggregate decoded estimates



Via the Plotkin decomposition, Recursive(ly) Project using all one-dimensional subspaces and Aggregate decoded estimates



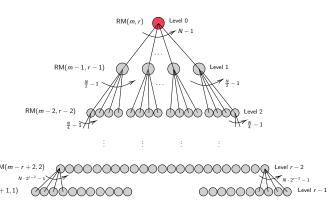
Repeat procedure over several iterations

A closer view of PA

Projection: For a received \mathbf{Y} , pick each one-dim. subspace \mathbb{B}_i in turn and construct

$$\mathbf{Y}_{/\mathbb{B}_i} := \left(Y_{/\mathbb{B}_i}(T): T \in \{0,1\}^m/\mathbb{B}_i\right),$$

where $Y_{/\mathbb{B}_i}(T) := \bigoplus_{\mathbf{b} \in \mathbb{B}_i} Y_{\mathbf{x} \oplus \mathbf{b}}$.

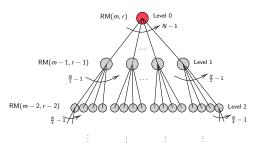


A closer view of PA

Aggregation: At a "parent node," for each $\mathbf{x} \in \{0,1\}^m$, compute

$$\phi(\mathbf{x}) = \sum_{i=1}^{N-1} \mathbb{1}\{Y_{/\mathbb{B}_i}([\mathbf{x} + \mathbb{B}_i]) \neq \widehat{Y}_{/\mathbb{B}_i}([\mathbf{x} + \mathbb{B}_i])\},$$

where $\widehat{Y}_{/\mathbb{B}_i} \leftarrow$ decoded estimate of a "child node". Flip $Y_{\mathbf{x}}$, if $\phi(\mathbf{x}) > \frac{N-1}{2}$.





Let
$$\overline{p}:=\frac{1}{2}\cdot(1-(1-2p)^{2^{r-2}})$$
 and $\eta(\overline{p}):=\frac{1}{2}\cdot(1-4\overline{p}(1-\overline{p})).$

Theorem

For any $0 < \epsilon < \eta(\overline{p})$, we have that for $r \ge 2$, using one-dimensional subspaces for projection,

$$P_{\mathsf{err}}^{\mathsf{RPA}}(\mathsf{RM}(m,r)) \leq 32 N^{r+1} \cdot \exp\left(-2^{-r-1} N \epsilon^2\right).$$

Let
$$\overline{p}:=\frac{1}{2}\cdot (1-(1-2p)^{2^{r-2}})$$
 and $\eta(\overline{p}):=\frac{1}{2}\cdot (1-4\overline{p}(1-\overline{p}))$.

Theorem

For any $0 < \epsilon < \eta(\overline{p})$, we have that for $r \ge 2$, using one-dimensional subspaces for projection,

$$P_{\mathsf{err}}^{\mathsf{RPA}}(\mathsf{RM}(m,r)) \leq 32 N^{r+1} \cdot \mathsf{exp}\left(-2^{-r-1} N \epsilon^2\right).$$

Corollary

For any
$$0 < \overline{c} < \frac{\log 2}{\log\left(\frac{1}{1-2D}\right)}$$
, we have that for all $r \leq \log(\overline{c}m)$,

$$\lim_{m\to\infty} P_{\rm err}^{\rm RPA}({\rm RM}(m,r))=0.$$

Let
$$\overline{p}:=\frac{1}{2}\cdot (1-(1-2p)^{2^{r-2}})$$
 and $\eta(\overline{p}):=\frac{1}{2}\cdot (1-4\overline{p}(1-\overline{p})).$ Further, let $p^{(j)}:=\frac{1}{2}\cdot \left(1-(1-2p)^{2^j}\right).$

Theorem

For any $0 < \epsilon < \eta(\overline{p})$, we have that for $r \ge 2$, using k-dimensional subspaces for projection, where k|(r-1),

$$P_{\text{err}}^{\text{RPA}}(\text{RM}(m,r)) \leq 64N^3 \cdot n_{k,m}^{\frac{r-1}{k}} \cdot \exp\left(-\ln\left(\frac{1-p^{(r-k-1)}}{p^{(r-k-1)}}\right) \cdot 2^{-r-1-k}N\epsilon^2\right).$$

Let
$$\overline{p}:=\frac{1}{2}\cdot (1-(1-2p)^{2^{r-2}})$$
 and $\eta(\overline{p}):=\frac{1}{2}\cdot (1-4\overline{p}(1-\overline{p})).$ Further, let $p^{(j)}:=\frac{1}{2}\cdot \left(1-(1-2p)^{2^j}\right).$

Theorem

For any $0 < \epsilon < \eta(\overline{p})$, we have that for $r \ge 2$, using k-dimensional subspaces for projection, where k|(r-1),

$$P_{\mathsf{err}}^{\mathsf{RPA}}(\mathsf{RM}(m,r)) \leq 64 N^3 \cdot n_{k,m}^{\frac{r-1}{k}} \cdot \exp\left(-\ln\left(\frac{1-p^{(r-k-1)}}{p^{(r-k-1)}}\right) \cdot 2^{-r-1-k} N\epsilon^2\right).$$

However, the rate guarantee $r \lesssim \log m$ does not change . . .

1. Via symmetry, it suffices to focus on $\mathbf{c} = \mathbf{0}$, since

$$P_{\text{err}}^{\text{RPA}}(\text{RM}(m,r)) = P_{\text{err}, 0}^{\text{RPA}}(\text{RM}(m,r)).$$

1. Via symmetry, it suffices to focus on $\mathbf{c} = \mathbf{0}$, since

$$P_{\text{err}}^{\text{RPA}}(\text{RM}(m,r)) = P_{\text{err}, 0}^{\text{RPA}}(\text{RM}(m,r)).$$

2. Restrict attention to the event where **one** iteration of RPA is sufficient for convergence:

$$\mathbf{Y} \xrightarrow{\mathsf{RPA}} \mathbf{0} \xrightarrow{\mathsf{RPA}} \mathbf{0} \xrightarrow{\mathsf{RPA}} \dots \xrightarrow{\mathsf{RPA}} \mathbf{0}.$$

1. Via symmetry, it suffices to focus on $\mathbf{c} = \mathbf{0}$, since

$$P_{\text{err}}^{\text{RPA}}(\text{RM}(m,r)) = P_{\text{err}, 0}^{\text{RPA}}(\text{RM}(m,r)).$$

Restrict attention to the event where one iteration of RPA is sufficient for convergence:

$$\mathbf{Y} \xrightarrow{\mathsf{RPA}} \mathbf{0} \xrightarrow{\mathsf{RPA}} \mathbf{0} \xrightarrow{\mathsf{RPA}} \dots \xrightarrow{\mathsf{RPA}} \mathbf{0}.$$

FHT Analyze error probability for the "base" case (r = 1).

Agg Analyze error probability upon aggregation, conditioned on all child nodes being decoded correctly.

1. Via symmetry, it suffices to focus on $\mathbf{c} = \mathbf{0}$, since

$$P_{\text{err}}^{\text{RPA}}(\text{RM}(m,r)) = P_{\text{err}, 0}^{\text{RPA}}(\text{RM}(m,r)).$$

Restrict attention to the event where one iteration of RPA is sufficient for convergence:

$$\mathbf{Y} \xrightarrow{\mathsf{RPA}} \mathbf{0} \xrightarrow{\mathsf{RPA}} \mathbf{0} \xrightarrow{\mathsf{RPA}} \dots \xrightarrow{\mathsf{RPA}} \mathbf{0}.$$

FHT Analyze error probability for the "base" case (r = 1).

Agg Analyze error probability upon aggregation, conditioned on **all child nodes** being decoded **correctly**.

We hence embark on the analysis of FHT and Agg for order-2 RM codes.

Elaborating on Step FHT

Via the simple map $x \mapsto (-1)^x$, for $x \in \{0,1\}$, we can view binary strings as ± 1 -vectors.

▶ For
$$\mathbf{s} \in \{0,1\}^m$$
, let $\chi_{\mathbf{s}} := ((-1)^{\mathbf{x} \cdot \mathbf{s}} : \mathbf{x} \in \{0,1\}^m)$. Then, $\{\mathbf{c} \in \mathsf{RM}(m,1)\} \mapsto \{\pm \chi_{\mathbf{s}} : \mathbf{s} \in \{0,1\}^m\}.$

Elaborating on Step FHT

Via the simple map $x \mapsto (-1)^x$, for $x \in \{0,1\}$, we can view binary strings as ± 1 -vectors.

- ▶ For $\mathbf{s} \in \{0,1\}^m$, let $\chi_{\mathbf{s}} := ((-1)^{\mathbf{x} \cdot \mathbf{s}} : \mathbf{x} \in \{0,1\}^m)$. Then, $\{\mathbf{c} \in \mathsf{RM}(m,1)\} \mapsto \{\pm \chi_{\mathbf{s}} : \mathbf{s} \in \{0,1\}^m\}$.
- ▶ Then, it can be argued that

$$\mathsf{FHT}(\mathbf{Y}_{/\mathbb{B}_i}) \equiv \underset{\pm \chi_\mathbf{s}}{\mathsf{argmax}} \langle \mathbf{Y}_{/\mathbb{B}_i}, \pm \chi_\mathbf{s} \rangle.$$

Elaborating on Step FHT

Via the simple map $x \mapsto (-1)^x$, for $x \in \{0,1\}$, we can view binary strings as ± 1 -vectors.

▶ For $\mathbf{s} \in \{0,1\}^m$, let $\chi_{\mathbf{s}} := ((-1)^{\mathbf{x} \cdot \mathbf{s}}: \mathbf{x} \in \{0,1\}^m)$. Then, $\{\mathbf{c} \in \mathsf{RM}(m,1)\} \mapsto \{\pm \chi_{\mathbf{s}}: \mathbf{s} \in \{0,1\}^m\}.$

▶ Then, it can be argued that

$$\mathsf{FHT}(\mathbf{Y}_{/\mathbb{B}_i}) \equiv \underset{\pm \chi_\mathbf{s}}{\mathsf{argmax}} \langle \mathbf{Y}_{/\mathbb{B}_i}, \pm \chi_\mathbf{s} \rangle.$$

▶ Via simple concentration of the inner products, this yields

Theorem

For all $\epsilon < \eta(p)$,

$$\Pr[\mathsf{FHT}(\mathbf{Y}_{/\mathbb{B}_i}) \neq \mathbf{0}] \leq 8N \cdot e^{-\frac{N\epsilon^2}{8}}.$$

See also [Burnashev-Dumer, T-IT 2006]

Conditioned on all child nodes being decoded correctly,

aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{N-1} (Y_{\mathbf{x}} \oplus Y_{\mathbf{x}+\mathbf{b}_i})$$

is
$$<$$
 or $> \frac{N-1}{2}$.

Conditioned on all child nodes being decoded correctly,

aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{N-1} (Y_{\mathbf{x}} \oplus Y_{\mathbf{x}+\mathbf{b}_i})$$

is < or $> \frac{N-1}{2}$.

 \triangleright since $\phi(\mathbf{x})$ concentrates around its mean,

$$\mathsf{Flip}(\mathbf{x}) = \mathbb{1}\left\{\overline{\phi}(\mathbf{x}) > \frac{1}{2}\right\} \approx \mathbb{1}\left\{\overline{\phi}_{\infty}(\mathbf{x}) > \frac{1}{2}\right\} = Y_{\mathbf{x}},$$

for large N, where $\overline{\phi}_{\infty}(\mathbf{x}) := p(1-Y_{\mathbf{x}}) + (1-p)Y_{\mathbf{x}}$.

Conditioned on all child nodes being decoded correctly,

aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{N-1} (Y_{\mathbf{x}} \oplus Y_{\mathbf{x}+\mathbf{b}_i})$$

is < or $> \frac{N-1}{2}$.

 \triangleright since $\phi(\mathbf{x})$ concentrates around its mean,

$$\mathsf{Flip}(\mathbf{x}) = \mathbb{1}\left\{\overline{\phi}(\mathbf{x}) > \frac{1}{2}\right\} \approx \mathbb{1}\left\{\overline{\phi}_{\infty}(\mathbf{x}) > \frac{1}{2}\right\} = Y_{\mathbf{x}},$$

for large N, where $\overline{\phi}_{\infty}(\mathbf{x}) := p(1-Y_{\mathbf{x}}) + (1-p)Y_{\mathbf{x}}$.

► Thus, we get

Theorem

For all $\epsilon < \eta(p)$,

$$\Pr[\mathsf{Flip} = \mathbf{Y}] \ge 1 - 32N^3 \cdot e^{-\frac{N\epsilon^2}{8}}.$$

Conditioned on all child nodes being decoded correctly,

aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{N-1} (Y_{\mathbf{x}} \oplus Y_{\mathbf{x}+\mathbf{b}_i})$$

is
$$<$$
 or $> \frac{N-1}{2}$.

 \triangleright since $\phi(\mathbf{x})$ concentrates around its mean,

$$\mathsf{Flip}(\mathbf{x}) = \mathbb{1}\left\{\overline{\phi}(\mathbf{x}) > \frac{1}{2}\right\} \approx \mathbb{1}\left\{\overline{\phi}_{\infty}(\mathbf{x}) > \frac{1}{2}\right\} = Y_{\mathbf{x}},$$

for large N, where $\overline{\phi}_{\infty}(\mathbf{x}) := p(1-Y_{\mathbf{x}}) + (1-p)Y_{\mathbf{x}}$.

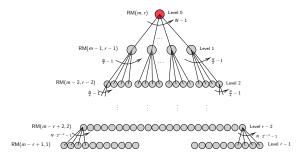
► Thus, we get

Theorem

For all $\epsilon < \eta(p)$,

$$\Pr{\overline{\mathbf{Y}} = \mathbf{0}} = \Pr{\left[\mathsf{Flip} = \mathbf{Y}\right]} \ge 1 - 32N^3 \cdot e^{-\frac{N\epsilon^2}{8}}.$$

Putting everything together



Projection-aggregation tree

Via recursive arguments on the projection-aggregation tree, we get

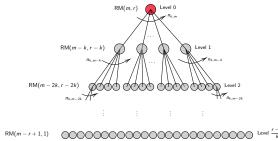
Theorem

For any $0 < \epsilon < \eta(\overline{p})$, we have that for $r \ge 2$, using one-dimensional subspaces for projection,

$$P_{\mathsf{err}}^{\mathsf{RPA}}(\mathsf{RM}(m,r)) \leq 32N^{r+1} \cdot \mathsf{exp}\left(-2^{-r-1}N\epsilon^2\right).$$

Projections using higher dimensional subspaces

▶ If projections are carried out using k-dimensional subspaces, for k > 1, then



the branching factor is

#k-dim. subspaces of
$$\{0,1\}^m = {m \brack k} := \prod_{i=0}^{k-1} \frac{2^m - 2^i}{2^k - 2^i} =: n_{k,m}.$$

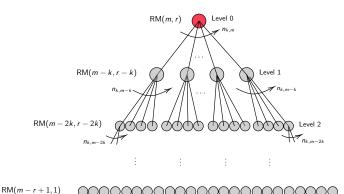
Then, conditioned on all children being decoded correctly, the concentration of $\phi(\mathbf{x})$ must be handled via more sophisticated concentration inequalities.

RPA, but using higher-dim. subspaces

Projection: For a received \mathbf{Y} , pick each k-dim. subspace \mathbb{B}_i in turn and construct

$$\mathbf{Y}_{/\mathbb{B}_i} := \left(Y_{/\mathbb{B}_i}(T) : T \in \{0,1\}^m / \mathbb{B}_i \right),$$

where $Y_{/\mathbb{B}_i}(T) := \bigoplus_{\mathbf{b} \in \mathbb{B}_i} Y_{\mathbf{x} \oplus \mathbf{b}}$.

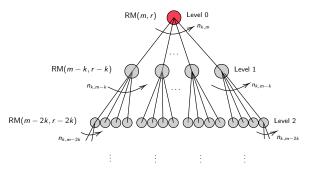


RPA, but using higher-dim. subspaces

Aggregation: At a "parent node," for each $\mathbf{x} \in \{0,1\}^m$, compute

$$\phi(\mathbf{x}) = \sum_{i=1}^{m_{\mathbf{x},m}} \mathbb{1}\{Y_{/\mathbb{B}_i}([\mathbf{x} + \mathbb{B}_i]) \neq \widehat{Y}_{/\mathbb{B}_i}([\mathbf{x} + \mathbb{B}_i])\}.$$

Flip $Y_{\mathbf{x}}$, if $\phi(\mathbf{x}) > \frac{n_{k,m}}{2}$.



RM(m-r+1,1)

 Conditioned on all child nodes being decoded correctly, aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{n_{k,m}} \bigoplus_{\mathbf{b} \in \mathbb{B}_i} Y_{\mathbf{x} \oplus \mathbf{b}},$$

is
$$<$$
 or $> \frac{n_{k,m}}{2}$.

 Conditioned on all child nodes being decoded correctly, aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{n_{\mathbf{k},m}} \bigoplus_{\mathbf{b} \in \mathbb{B}_i} Y_{\mathbf{x} \oplus \mathbf{b}},$$

is
$$<$$
 or $> \frac{n_{k,m}}{2}$.

▶ Concentration of $\phi(\mathbf{x})$ about its mean, however, needs a more sophisticated result:

Theorem (Raginsky-Sason (2018), Thm. 3.4.4)

Let X_1, \ldots, X_n be i.i.d. Ber(q) random variables. Then, for every Lipschitz function $f: \{0,1\}^n \to \mathbb{R}$ with Lipschitz constant c_f , we have for all $\alpha > 0$,

$$\Pr[f(X^n) - \mathbb{E}[f(X^n)] > \alpha] \le \exp\left(-\ln\left(\frac{1-q}{q}\right) \cdot \frac{\alpha^2}{nc_f^2 \cdot (1-2q)}\right).$$

 Conditioned on all child nodes being decoded correctly, aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{n_{k,m}} \bigoplus_{\mathbf{b} \in \mathbb{B}_i} Y_{\mathbf{x} \oplus \mathbf{b}},$$

is
$$<$$
 or $> \frac{n_{k,m}}{2}$.

An explicit computation of the Lipschitz constant c_f associated with ϕ , seen as a function of $(Y_{\mathbf{x} \oplus \mathbf{b}})$, then results in

$$\mathsf{Flip}(\mathbf{x}) = \mathbb{1}\left\{\overline{\phi}(\mathbf{x}) > \frac{1}{2}\right\} \approx \mathbb{1}\left\{\overline{\phi}_{\infty}(\mathbf{x}) > \frac{1}{2}\right\} = Y_{\mathbf{x}},$$

for large N, for a suitably defined $\overline{\phi}_{\infty}(\mathbf{x})$.

Theorem

For all ϵ smaller than a suitable function of p,

$$\Pr[\mathsf{Flip} = \mathbf{Y}] \geq 1 - \delta_m$$

for an explicitly computable $\delta_m \xrightarrow{m \to \infty} 0$.

 Conditioned on all child nodes being decoded correctly, aggregation reduces to checking if

$$\phi(\mathbf{x}) = \sum_{i=1}^{n_{\mathbf{k},m}} \bigoplus_{\mathbf{b} \in \mathbb{B}_i} Y_{\mathbf{x} \oplus \mathbf{b}},$$

is
$$<$$
 or $> \frac{n_{k,m}}{2}$.

▶ An explicit computation of the Lipschitz constant c_f associated with ϕ , seen as a function of $(Y_{\mathbf{x} \oplus \mathbf{b}})$, then results in

$$\mathsf{Flip}(\mathbf{x}) = \mathbb{1}\left\{\overline{\phi}(\mathbf{x}) > \frac{1}{2}\right\} \approx \mathbb{1}\left\{\overline{\phi}_{\infty}(\mathbf{x}) > \frac{1}{2}\right\} = Y_{\mathbf{x}},$$

for large N, for a suitably defined $\overline{\phi}_{\infty}(\mathbf{x})$.

Theorem

For all ϵ smaller than a suitable function of p,

$$\Pr\left[\overline{\mathbf{Y}} = \mathbf{0}\right] = \Pr\left[\mathsf{Flip} = \mathbf{Y}\right] \ge 1 - \delta_m,$$

for an explicitly computable $\delta_m \xrightarrow{m \to \infty} 0$.

Further extensions

1. Can we extend similar analysis to general BMS channels?

2. Can RPA decoding be made more efficient by using a subset of subspaces for projection?

Ongoing work with







Dorsa Fathollahi (PhD, Stanford U.), Harshithanjani Athi (PhD, UT Austin), Lalitha Vadlamani (IIIT-H)

