Format of challenges

The decodingchallenge team

August 14, 2019

Contents

1 The Syndrome Decoding challenge

Notation. Formally, a Syndrome Decoding[1] challenge consists in a tuple $(n, w, \mathbf{H}, \mathbf{s})$, where:

- $n \geq 2$ is an integer.
- $w = d_{\mathrm{GV}}(n, n/2)$ is the target weight.
- $\mathbf{H} \in \mathbb{F}_q^{n/2 \times n}$ is the parity-check matrix. We assume that $\mathbf{H}$ is structured as follows:

  $$\mathbf{H} = [\mathbf{I}_{n/2} | \mathbf{M}^\top],$$

  where $\mathbf{I}_{n/2}$ denotes the identity matrix of size $n/2$, and $\mathbf{M}^\top \in \mathbb{F}_2^{n/2 \times n/2}$ is the transpose of a random matrix $\mathbf{M}$. For each $1 \leq i \leq n/2$, let us denote by $\mathbf{m}_i \in \mathbb{F}_2^{n/2}$ the i-th row of $\mathbf{M}$, so that:

  $$\mathbf{H} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & & & & & \\ 0 & 1 & \ddots & & 0 & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & 0 & \mathbf{m}_1^\top & \mathbf{m}_2^\top & \cdots & \cdots & \mathbf{m}_{n/2}^\top \\ \vdots & & \ddots & \ddots & 0 & \vdots & \vdots & & & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & & & & & \end{pmatrix}.$$
- $\mathbf{s} \in \mathbb{F}_2^{n/2}$ is a random syndrome.

The goal of the challenge is to produce a word $\mathbf{e}$ of Hamming weight $\leq w$ such that $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$.

Format of files. Each file is named `SD_<n>_<seed>`, where

- `<n>` is the length n;
- `<seed>` is the random seed used in order to generate the challenge.

It is structured as follows:

- line 1: a comment
- line 2: the length n
- line 3: a comment
- line 4: the seed
- line 5: a comment
- line 6: the target weight w
- line 7: a comment
- line 8: the 1st row $\mathbf{m}_1$ of $\mathbf{M}$, given as a string of length $n/2$; the j-st character is either `0` or `1`, and corresponds to the j-th bit of $\mathbf{m}_1$
- line 9: the 2nd row $\mathbf{m}_2$ of $\mathbf{M}$
- ...
- line 7 + $n/2$: the last row $\mathbf{m}_{n/2}$ of $\mathbf{M}$
- line 8 + $n/2$: a comment
- line 9 + $n/2$: the syndrome $\mathbf{s}$, given as a binary string of length $n/2$.

2 The Low-weight Codeword challenge

Notation. Formally, a Low-weight Codeword[2] challenge consists in a tuple $(n, \mathbf{H})$, where:

[1] `https://decodingchallenge.inria.fr/syndrome/`

[2] `https://decodingchallenge.inria.fr/low-weight/`

- $n \geq 2$ is an integer.
- $\mathbf{H} \in \mathbb{F}_q^{n/2 \times n}$ is the parity-check matrix. We assume that $\mathbf{H}$ is structured as follows:

$$\mathbf{H} = [\mathbf{I}_{n/2} | \mathbf{M}^\top],$$

  where $\mathbf{I}_{n/2}$ denotes the identity matrix of size $n/2$, and $\mathbf{M}^\top \in \mathbb{F}_2^{n/2 \times n/2}$ is the transpose of a random matrix $\mathbf{M}$. For each $1 \leq i \leq n/2$, let us denote by $\mathbf{m}_i \in \mathbb{F}_2^{n/2}$ the i-th row of $\mathbf{M}$, so that:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & & & & & \\ 0 & 1 & \ddots & & 0 & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & 0 & \mathbf{m}_1^\top & \mathbf{m}_2^\top & \cdots & \cdots & \mathbf{m}_{n/2}^\top \\ \vdots & & \ddots & \ddots & 0 & \vdots & \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 & 1 & & & & & \end{pmatrix}.$$

The goal of the challenge is to produce a non-zero codeword $\mathbf{e}$ (*i.e.* a binary vector satisfying $\mathbf{He}^\top = \mathbf{0}$) whose Hamming weight is lowest as possible.

Format of files. Each file is named `LW_<n>_<seed>`, where

- `<n>` is the length n;
- `<seed>` is the random seed used in order to generate the challenge.

It is structured as follows:

- line 1: a comment
- line 2: the length n
- line 3: a comment
- line 4: the seed
- line 5: a comment
- line 6: the 1st row $\mathbf{m}_1$ of $\mathbf{M}$, given as a string of length $n/2$; the j-st character is either `0` or `1`, and corresponds to the j-th bit of $\mathbf{m}_1$
- line 7: the 2nd row $\mathbf{m}_2$ of $\mathbf{M}$
- ...
- line 5 + $n/2$: the last row $\mathbf{m}_{n/2}$ of $\mathbf{M}$.

3 The Goppa-McEliece Syndrome Decoding challenge

Notation. Formally, a syndrome decoding challenge in the Goppa-McEliece setting[3] consists in a tuple $(n, w, \mathbf{H}, \mathbf{s})$, where:

- $n \geq 2$ is an integer.
- $k = \lceil 0.8n \rceil$ (in the specification of the Classic McEliece cryptosystem, $R \approx 0.7968$).
- $w = \lceil \frac{n}{\lceil 5 \log_2 n \rceil} \rceil$ is the target weight.
- $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ is the parity-check matrix. We assume that $\mathbf{H}$ is structured as follows:

$$\mathbf{H} = [\mathbf{I}_{n-k} | \mathbf{M}^\top],$$

  where $\mathbf{I}_{n-k}$ denotes the identity matrix of size $n-k$, and $\mathbf{M}^\top \in \mathbb{F}_2^{(n-k) \times k}$ is the transpose of a random matrix $\mathbf{M}$. For each $1 \leq i \leq k$, let us denote by $\mathbf{m}_i \in \mathbb{F}_2^{n-k}$ the i-th row of

[3] `https://decodingchallenge.inria.fr/goppa/`

M, so that:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & \dots & \vdots & \vdots & & & \vdots \\ 0 & \ddots & 0 & \mathbf{m}_1^\top & \mathbf{m}_2^\top & \cdots & \cdots & \mathbf{m}_k^\top \\ \vdots & 0 & 1 & \vdots & \vdots & & & \vdots \end{pmatrix}.$$

- $\mathbf{s} \in \mathbb{F}_2^{n-k}$ is a syndrome produced by a random error $\mathbf{e}$ of Hamming weight w (*i.e* $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$).

The goal of the challenge is to produce a word $\mathbf{e}'$ of Hamming weight $\leq w$ such that $\mathbf{H}\mathbf{e}'^\top = \mathbf{s}^\top$.

Format of files. Each file is named `Goppa_<n>`, where

- `<n>` is the length n,

and has been built by a trusted institution which erased the secret value $\mathbf{e}$. You can choose your favorite provider on the right banner of the website.

Each file is structured as follows:

- line 1: a comment
- line 2: the length n
- line 3: a comment
- line 4: the dimension $k = \lceil 0.8n \rceil$
- line 5: a comment
- line 6: the target weight w
- line 7: a comment
- line 8: the 1st row $\mathbf{m}_1$ of $\mathbf{M}$, given as a string of length $n-k$; the j-st character is either `0` or `1`, and corresponds to the j-th bit of $\mathbf{m}_1$
- line 9: the 2nd row $\mathbf{m}_2$ of $\mathbf{M}$
- ...
- line 7 + k: the last row $\mathbf{m}_k$ of $\mathbf{M}$
- line 8 + k: a comment
- line 9 + k: the syndrome $\mathbf{s}$, given as a binary string of length $n-k$.

4 The Quasi-cyclic Syndrome Decoding challenge

Notation. Formally, a syndrome decoding challenge in the Quasi-cyclic setting[4] consists in a tuple $(n, w, \mathbf{H}, \mathbf{s})$, where:

- $w \geq 2$ is an integer corresponding to the target.
- $n = w^2$.
- $k = \lceil n/2 \rceil$.
- $\mathbf{H} \in \mathbb{F}_q^{n-k \times n}$ is the parity-check matrix. We assume that $\mathbf{H}$ is structured as follows:

$$\mathbf{H} = [\mathbf{I}_{n-k} | \mathbf{M}^\top],$$

where $\mathbf{I}_{n-k}$ denotes the identity matrix of size $n-k$, and $\mathbf{M}^\top \in \mathbb{F}_2^{(n-k)\times k}$ is the transpose of a random circulant matrix $\mathbf{M}$. Precisely, the matrix $\mathbf{M}^\top$ is determined by $n/2$ bits

[4] `https://decodingchallenge.inria.fr/q-c/`

$(m_1, \dots, m_{n/2})$, and has the following form:

$$\mathbf{M}^\top = \begin{pmatrix} m_1 & m_2 & \cdots & \cdots & m_{n/2-1} & m_{n/2} \\ m_{n/2} & m_1 & m_2 & \cdots & \cdots & m_{n/2-1} \\ & \ddots & \ddots & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ & & & \ddots & \ddots & m_2 \\ m_2 & \cdots & \cdots & m_{n/2-1} & m_{n/2} & m_1 \end{pmatrix}.$$

Let us define $\mathbf{h} = (m_1, m_{n/2}, m_{n/2-1}, \dots, m_2) \in \mathbb{F}_2^{n/2}$ to be the first column of $\mathbf{M}^\top$, and denote by $\sigma^i(\mathbf{h})$ its i-th shift $(m_{1+i}, m_{n/2+i}, \dots, m_{2+i})$, where indices are taken modulo $n/2$ and lie in $\{1, \dots, n/2\}$. Then $\mathbf{H}$ can actually be written:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & & & & & \\ 0 & 1 & \ddots & & 0 & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & 0 & \mathbf{h}^\top & \sigma(\mathbf{h})^\top & \sigma^2(\mathbf{h})^\top & \cdots & \sigma^{n/2-1}(\mathbf{h})^\top \\ \vdots & & \ddots & \ddots & 0 & \vdots & \vdots & & & \vdots \\ 0 & \dots & \dots & 0 & 1 & & & & & \end{pmatrix}.$$

- $\mathbf{s} \in \mathbb{F}_2^{n/2}$ is a syndrome produced by a random error $\mathbf{e}$ of Hamming weight w (*i.e* $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$).

The goal of the challenge is to produce a word $\mathbf{e}'$ of Hamming weight $\leq w$ such that $\mathbf{H}\mathbf{e}'^\top = \mathbf{s}^\top$.

Format of files. Each file is named `QC_<n>`, where

- `<n>` is the length n,

and has been built by a trusted institution which erased the secret value **e**. You can choose your favorite provider on the right banner of the website.

Each file is structured as follows:

- line 1: a comment
- line 2: the length n
- line 3: a comment
- line 4: the target weight w
- line 5: a comment
- line 6: the vector **h**, given as a binary string of length $n/2$
- line 7: a comment
- line 8: the syndrome **s**, given as a binary string of length $n/2$.