About the Failure Probability of Syndrome Decoding

the `decodingchallenge` team

August 14, 2019

1 Introduction

Given n we define $k = \lfloor \frac{n}{2} \rfloor$ and $w = \lceil 1.05 \times d_{GV} \rceil$ where d_{GV} denotes the Gilbert Varshamov bound, defined as follows.

$$d_{GV}(n,k) = \min \left\{ d \in \mathbb{N} \mid \sum_{j=0}^{d-1} \binom{n}{j} \geq 2^{n-k} \right\}.$$

2 Failure Probability

We want to calculate (or at least give an upper bound to) the probability that a random binary linear code of length n and dimension k (defined by its parity-check matrix $\boldsymbol{H}$) has no solution $\boldsymbol{e}$ of weight w to the problem $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal$, for a fixed vector $\boldsymbol{s}$.

Let $\mathcal{C}_{n,k}$ be the set of random binary linear codes of length n and dimension k and denote X the random variable defined over $\mathcal{C}_{n,k}$ that counts the number of solutions of weight w to the equation $\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal$.

We want to bound $\mathbf{Prob}_{\boldsymbol{H} \in \mathcal{C}_{n,k}}(X = 0)$.

3 Computation

We have $X = \sum_{\boldsymbol{e} \in \mathbb{F}_2^n, |\boldsymbol{e}|=w} \mathbf{1}_{\{\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal\}}$. Therefore $\mathbb{E}\{X\} = \binom{n}{w} 2^{-(n-k)}$.

We make use of Chebyshev's inequality: for X a random variable with finite expected value $\exp X$ and finite non–zero variance $\mathrm{Var}\{X\}$, for any $\varepsilon > 0$ we have

$$\mathbf{Prob}\left(|X - \exp X| \geq \varepsilon\right) \leq \frac{\mathrm{Var}\{V\}}{\varepsilon^2}.$$

In our case we have

$$\begin{aligned}
\mathrm{Var}\{X\} &= \binom{n}{w}\mathrm{Var}\left\{\mathbf{1}_{\{\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal\}}\right\} \\
&= \binom{n}{w}(\mathbb{E}\left\{\mathbf{1}^2_{\{\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal\}}\right\} - \mathbb{E}\left\{\mathbf{1}_{\{\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal\}}\right\}^2) \\
&= \binom{n}{w}(\mathbb{E}\left\{\mathbf{1}_{\{\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal\}}\right\} - \mathbb{E}\left\{\mathbf{1}_{\{\boldsymbol{H}\boldsymbol{e}^\intercal = \boldsymbol{s}^\intercal\}}\right\}^2) \\
&= \binom{n}{w}(\frac{1}{2^{n-k}} - \frac{1}{2^{2(n-k)}}) \\
&= \binom{n}{w}\frac{1}{2^{n-k}}(1 - \frac{1}{2^{n-k}}).
\end{aligned}$$

We can now write

$$\begin{aligned}
\mathbf{Prob}(X = 0) &< \mathbf{Prob}\left(|X - \exp X| \geq \frac{\mathbb{E}\{X\}}{2}\right) \\
&\leq 4\frac{\mathbb{E}\{X\}}{\mathrm{Var}\{X\}^2} \\
&\leq \frac{2^{n-k+2}}{\binom{n}{w}}.
\end{aligned} \tag{1}$$

4 Conclusions

The choice of $w = \lceil (1+\alpha) \times d_{GV} \rceil$ for some $\alpha > 0$ (in our case $\alpha = 0.05$) ensures that asymptotically $\binom{n}{w}$ grows faster than 2^{n-k} and therefore $\mathbf{Prob}(X = 0) \rightarrow_{n\rightarrow\infty} 0$. We can easily compute the value of the bound on $\mathbf{Prob}(X = 0)$ for a given value of n.

n	value of (1)
10	$2^{-0.714}$
20	$2^{-1.92}$
50	$2^{-4.222}$
100	$2^{-3.294}$
200	$2^{-8.595}$
300	$2^{-8.612}$
400	$2^{-11.372}$
500	$2^{-11.342}$
600	$2^{-14.151}$
700	$2^{-14.121}$
800	$2^{-16.961}$
900	$2^{-19.813}$
1000	$2^{-19.797}$

Figure 1: Some values of the bound