Syndrome Decoding and Error Correction for Quantum Key Distribution

Rasmus Päivärinta

rasmus.paivarinta@tkk.fi

Syndrome Decoding

The simplest way to correct errors is to compute the Hamming distance from the received word to all codewords. A better and faster way will be presented.

Scenario

Alice sends the codeword c to Bob who receives r.
Now we can write

$$\vec{r} = \vec{c} + \vec{e}$$

where $\vec{e} \in F^n$ is the error vector.

- A reasonable channel is assumed, and hence $\omega(e)$ is small.

Definition of Coset

Let $C \subseteq F^n$ be a linear code and $\vec{x} \in F^n$. The coset $\vec{x} + C$ is defined as

$$\vec{x} + C = \{\vec{x} + \vec{c} \mid \vec{c} \in C\}.$$

Definition of Syndrome

Let $C \subseteq F^n$ be an $[n, k]$ linear code and H a *check matrix* for C. Then

$$\vec{s} = H\vec{r}^T \in F^{n-k}$$

is the *syndrome* of $\vec{r}$.

Syndrome Decoding

- Bob receives $\vec{r} = \vec{c} + \vec{e}$. Now, $\vec{r}$ and $\vec{e}$ have the same syndrome iff $H\vec{r}^T = H\vec{e}^T$, which is true iff $H(\vec{r} - \vec{e})^T = \vec{0}$, which is true iff $\vec{r} - \vec{e} \in C$.
- Bob knows $\vec{r} - \vec{e} = \vec{c} \in C$. It follows that $\vec{r}$ and $\vec{e}$ must have the same syndrome. Bob wants to find a word $\vec{e}$ with small weight such that $\vec{e}$ has the same syndrome as $\vec{r}$.
- Two words have the same sydrome iff they are in the same coset.

Error Correction for QKD

Background

After the *Bennett-Brassard* key distribution scheme Alice and Bob would have obtained identical keys in an ideal world. In reality further processing is needed to confirm this.

- Unlike in classical communication, errors in the signal might be the effect of an eavesdropper.
- Error correction is applied after all the data is transmitted.

Error Correction Using Syndromes

Suppose Alice and Bob have bit strings

$$\vec{a} = (a_1, a_2, a_3, a_4, a_5, a_6, a_7) \vec{b} = (b_1, b_2, b_3, b_4, b_5, b_6, b_7)$$

and they are confident that their string differ in at most one place.

1. Alice and Bob agree publicly on a check matrix H for the binary $[7, 4]$ Hamming code

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Error Correction Using Syndromes

2. Alice uses H to $\vec{a}^T$ to get $\vec{s}^A = H\vec{a}^T$ and sends $\vec{s}^T$ to Bob.
3. Bob computes $\vec{s}^B = H\vec{b}^T$.
4. Bob computes $\vec{s} = \vec{s}^B - \vec{s}^A = H\vec{b}^T - H\vec{a}^T = H(\vec{b} - \vec{a})^T$. Let $\vec{e} = \vec{b} - \vec{a}$. Then $\vec{s} = H\vec{e}^T$.
5. If indeed there is no more than one error in the string of seven bits, then $\omega(\vec{e}) \leq 1$, then there is a unique minimun-weight vector $\vec{v}$ that satisfies $H\vec{v}^T = \vec{s}$ and that vector must be $\vec{e}$.
6. Bob now replaces his string $\vec{b}$ with the corrected version $\vec{b} - \vec{e}$.

Syndrome Correction Example

Suppose $\vec{a} = (100011)$ and $\vec{b} = (1100111)$. Then

$$H\vec{a}^T = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \qquad H\vec{b}^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \qquad \vec{s} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

now $\vec{e} = (0100000)$, and Bob replaces $\vec{b}$ with $\vec{b} - \vec{e} = (1100111) - (0100000) = (1000111)$, which equals $\vec{a}$.

Error Correction Using Parity Checks

1. Alice and Bob publicly share a random permutation to distribute errors over the string.
2. Both divide their strings into blocks. The length of blocks is chosen so that it is unlikely that a block contains more than one error.
3. For each block, Alice and Bob compute and compare the parity of the block. Blocks for which the parities match are accepted as correct.

Error Correction Using Parity Checks

4. For each other block, the block is divided into two subblocks and they are compared until an error is found.
5. The whole process is repeated several times varying the random permutation. In each round, the starting block size will be longer since fewer errors remain.
6. Once the block size is about the length of the whole bit string, different strategy is used. Random subset of size approximately half of the whole string is chosen and parities for the subsets are compared as before. This is repeated until several successive repetitions have uncovered no more errors.

Parity Check Example

Suppose Alice's and Bob's strings are

$\vec{a} = (11011001) \qquad \vec{b} = (11011011)$

Final words

After the error correction, Alice and Bob need to estimate how much information Eve has possibly gained from *monitoring the original quantum transmission* and from *public communication* $\longrightarrow$ privacy amplification.