Exercises

- What is the probability that a random $m \times n$ matrix over $\mathbb{F}_q$ is full rank?
- Prove that the dimension of $\Gamma(L, g)$ with $\deg(g) = t$ is at least $n - mt$.
- Implement one of the ISD algorithms and figure out how many iterations it takes.
- How can we perform the Verheul–Doumen–Tilborg attack against Niederreiter? What if the decoder only works when $\mathrm{wt}(e) = t$?
- Convince yourself that the decapsulation algorithm of Classic McEliece returns $\mathrm{Hash}_{32}(0, s, c)$ with an overwhelming probability if the ciphertext is modified.
- Suppose we have a decoder that, given He with $\mathrm{wt}(e) = t$, always returns e. The output is undefined for other inputs. How can we tell whether the input is valid or not?