Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Network Coding

IN2315, WiSe 2023/23

Tutorial 4

July 26, 2024

Problem 1 Linear Network Coding

We consider the finite extension field $F_q[x]$ with $q = 3^2 = 9$ and the reduction polynomial $r(x) = x^2 + 1$.
Hint: Use the addition and multiplication table from Tutorial 1.

For communication, we use generations of size 3. Assume you receive the following packets, each consisting of its coding vector followed by a coded payload:

$$x_1^T = 02\ 12\ 22 \quad 01\ 01\ 01$$
$$x_2^T = 11\ 00\ 22 \quad 12\ 12\ 12$$
$$x_3^T = 10\ 11\ 10 \quad 10\ 11\ 12$$

a)* Under which condition can you decode the original packets a_1, a_2, and a_3?

If the coding vctors c_1, c_2, and c_3 are linearly independent, decoding is possible.

b)* Decode the original packets a_1, a_2 and a_3

$$\left[\begin{array}{ccc|ccc} 02 & 12 & 22 & 01 & 01 & 01 \\ 11 & 00 & 22 & 12 & 12 & 12 \\ 10 & 11 & 10 & 10 & 11 & 12 \end{array}\right] \quad x_1' = 02 \cdot x_1$$

$$\left[\begin{array}{ccc|ccc} 01 & 21 & 11 & 02 & 02 & 02 \\ 11 & 00 & 22 & 12 & 12 & 12 \\ 10 & 11 & 10 & 10 & 11 & 12 \end{array}\right] \quad x_2' = x_2 + 22 \cdot x_1'$$

$$\left[\begin{array}{ccc|ccc} 01 & 21 & 11 & 02 & 02 & 02 \\ 00 & 01 & 02 & 20 & 20 & 20 \\ 00 & 00 & 01 & 20 & 21 & 22 \end{array}\right] \quad x_1'' = x_1' + 12 \cdot x_2', \quad x_3' = x_3 + 20 \cdot x_1'$$

$$\left[\begin{array}{ccc|ccc} 01 & 00 & 02 & 10 & 10 & 10 \\ 00 & 01 & 02 & 20 & 20 & 20 \\ 00 & 00 & 01 & 20 & 21 & 22 \end{array}\right] \quad x_2'' = x_2' + x_3', \quad x_1''' = x_1'' + x_3'$$

$$\left[\begin{array}{ccc|ccc} 01 & 00 & 00 & 00 & 01 & 02 \\ 00 & 01 & 00 & 10 & 11 & 12 \\ 00 & 00 & 01 & 20 & 21 & 22 \end{array}\right]$$

$$a_1 = 00\ 01\ 02$$
$$a_2 = 10\ 11\ 12$$
$$a_3 = 20\ 21\ 22$$

Prof. Dr.-Ing. Stephan Günther Stephan Günther
guenther@tum.de nc@net.in.tum.de

Problem 2 Random Linear Network Coding

We consider the finite field $\mathbb{F}_2$ and a generation size of 4.

a)* Compute the probability that two random coding vectors $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ are linear independent.

$$\begin{aligned}\Pr\left[\dim\{\boldsymbol{c}_1, \boldsymbol{c}_2\} = 2\right] &= \left(1 - \frac{2^0}{2^4}\right)\left(1 - \frac{2^1}{2^4}\right) \\ &= \left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{8}\right) \\ &= \frac{15}{16} \cdot \frac{7}{8} \\ &= \frac{105}{128} \\ &\approx 0.82\end{aligned}$$

b)* Compute the probability that four received coded packets with randomly chosen coding vectors $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$ and $\boldsymbol{c}_4$ are fully decodable.

$$\begin{aligned}\Pr\left[\dim\{\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \boldsymbol{c}_4\} = 4\right] &= \left(1 - \frac{2^0}{2^4}\right)\left(1 - \frac{2^1}{2^4}\right)\left(1 - \frac{2^2}{2^4}\right)\left(1 - \frac{2^3}{2^4}\right) \\ &= \left(1 - \frac{1}{16}\right)\left(1 - \frac{1}{8}\right)\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{2}\right) \\ &= \frac{15}{16} \cdot \frac{7}{8} \cdot \frac{3}{4} \cdot \frac{1}{2} \\ &= \frac{315}{1024} \\ &\approx 0.308\end{aligned}$$

We now consider a general galois field F_q with q elements and a generation size of N.

c) State the general formula to compute the probability that N randomly chosen coding vectors form the complete N-dimensional vector space.

$$\Pr\left[\dim \bigcup_{i=1}^{N} \{\boldsymbol{c}_i\} = N\right] = \prod_{i=1}^{N}\left(1 - \frac{q^{i-1}}{q^N}\right)$$

d) Find a lower bound of the above probability for arbitrary N. *Hint:* Have a look at the Euler function ϕ.

Prof. Dr.-Ing. Stephan Günther guenther@tum.de
Stephan Günther nc@net.in.tum.de

$$\begin{aligned}\Pr\left[\dim \bigcup_{i=1}^{N} \{\boldsymbol{c}_i\} = N\right] &= \prod_{i=1}^{N} \left(1 - \frac{q^{i-1}}{q^N}\right) \\ &\geq \prod_{i=1}^{\infty} \left(1 - q^{-i}\right) \\ &= \phi\left(\frac{1}{q}\right)\end{aligned}$$

e) Compute the above bound for $q \in \{2, 4, 16, 256\}$ with e. g. Matlab.

$$\begin{aligned}\phi\left(\frac{1}{2}\right) &\approx 0.289 \\ \phi\left(\frac{1}{4}\right) &\approx 0.689 \\ \phi\left(\frac{1}{16}\right) &\approx 0.934 \\ \phi\left(\frac{1}{256}\right) &\approx 0.996\end{aligned}$$

Problem 3 FEC with ARQ

Consider a simple wireless network consisting of two nodes s and t. Node s transmits packets of $l = 15\,808$ bit each. The channel has a bit error rate of $\epsilon = 10^{-4}$.

If a transmission of s is successfully received by t, an acknowledgement is triggered and sent back to s. We assume orthogonal scheduling, i. e, there are no additional losses due to collisions. Further we assume that acknowledgements do not get lost.

a)* Let X be a random variable that counts the number of bit errors in a given packet. Determine the probability for a successful transmission, i. e., $\Pr[X = 0]$.

$X \sim \text{Bin}(l, \epsilon)$ and therefore

$$\Pr[X = i] = \binom{l}{i} \epsilon^i (1-\epsilon)^{l-i} \text{ and}$$
$$\Pr[X = 0] = (1-\epsilon)^{1976 \cdot 8} = 20.58\,\%.$$

b) Let T denote a random variable that counts the number of transmissions until a packet is acknowledged. Determine $\Pr[T = i]$ and $\Pr[T \leq i]$ in general and for $i = 7$.

$T \sim \text{Geo}(p)$ with $p = \Pr[X = 0]$ and therefore

$$\Pr[T = i] = (1-p)^{i-1} p,$$
$$\Pr[T \leq i] = \sum_{m=1}^{i} \Pr[T = m] = 1 - (1-p)^i, \text{ and}$$
$$\Pr[T \leq 7] = 80.07\,\%$$

c) Determine the expectation $\mathrm{E}[T]$, i. e., the average number of transmissions that are needed until successful reception.

$T \sim \text{Geo}(p)$ with $p = \Pr[X = 0]$ and therefore

$$\mathrm{E}[T] = \frac{1}{p} = 4.86.$$

To secure transmissions node s now employs a FEC code which maps source symbols of $k = 247$ bit to coded symbols of $n = 255$ bit. The code is able to detect and correct a single bit-error in each coded symbol.

d) Determine the probability that a single symbol can be recovered at the receiver.

$$\begin{aligned}\Pr[X \leq 1] &= \sum_{i=0}^{1} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i} \\ &= (1-\epsilon)^n + n\epsilon(1-\epsilon)^{n-1} \\ &= 99.97\,\%\end{aligned}$$

e) Let Z count the number of incorrect transmitted symbols. Determine the probability for a successful transmission during the first attempt for the whole packet if FEC is used.

A packet is split into $m = \frac{l \cdot 8}{k} = 64$ symbols. The probability that an individual symbol can be recovered is $q = 99.97\,\%$ and the error probability is therefore $1 - q$. Then we have $Z \sim \mathrm{Bin}(m, 1-q)$ and therefore

$$\Pr[Z = i] = \binom{m}{i} (1-q)^i q^{m-i} \text{ and}$$
$$\Pr[Z = 0] = q^m \approx 98.10\,\%.$$