Codetheorie - Encyclopedia Academia

Codetheorie	
Richting	WiskundeBachelor Informatica KeuzevakkenInformatica
Jaar	2BWIS

Academiejaar 2021-2022

1. Wat is het Index Calculus Algoritme, waarvoor dient het en hoe en waarom werkt het?
2. Beschrijf kort de werking en de verschillende stappen van Rijndael.
3. Wat is de Hamming square code en geef hoeveel fouten deze code kan detecteren en corrigeren. Is dit een lineaire code? Veronderstel dat je een woord ontvangt met enen, wat zijn dan alle codewoorden die het dichtst bij dit ontvangen woord zijn?
4. Toon aan dat de Hamming code Ham(r,q) een perfecte [qr−1q−1,qr−1q−1−r,3][qr−1q−1,qr−1q−1−r,3] -code is voor FqFq (indien voor qq niet lukt mag je voor q=2q=2 bewijzen.)
5.
    1. Beschrijf het algoritme van Berlekamp-Massey-Fourney voor Reed-Solomon-codes, definieer daarbij de variabelen die je gebruikt.
    2. We werken met F16F16 die 1 fout verbeterend is, met primitief element αα dat een wortel is van x4−x+1x4−x+1. Bepaal de generator polynoom.
    3. Pas het in 5)1) beschreven algoritme toe om het volgende ontvangen bericht te decoderen [α12,α5,α,1,α4,0,α,α7,α,0,α4,1,α,α5,α12][α12,α5,α,1,α4,0,α,α7,α,0,α4,1,α,α5,α12]. Wat was de verzonden (ongecodeerde) boodschap?

Academiejaar 2020-2021

1. In deze vraag kijken we naar het El Gamal versleutelingsprotocol. Hoe werkt het? Waarom is dit wiskundig correct? Op welke one way functie(s) is dit gebaseerd?
2. Elliptische krommen
    1. Beschrijf hoe de optelling en de (scalaire) vermenigvuldiging wordt gedefinieerd op een elliptische kromme. (Geef meetkundige uitleg en formules).
    2. Beschouw volgende elliptische kromme
    y2=x3+3x+3(mod29)
    y2=x3+3x+3(mod29)
    Bereken 2P2P en 3P3P voor P=(1,6)P=(1,6). (Optellings- en vermenigvuldigingstabel mod 29 gegeven)
3. Hamming codes
    1. Geef de parameters van Ham(r,2)Ham(r,2) en toon ze aan.
    2. Bewijs dat Ham(r,2)Ham(r,2) perfect is.
    3. Geef het aantal codewoorden met gewicht 3 in Ham(r,2)Ham(r,2). (Dit staat niet in de cursus, maar is te beredeneren.)
4. Reed-Solomon codes
    1. Geef het Berlekamp-Massey-Fourney algoritme voor Reed-Solomon codes, geef definities van gebruikte variabelen (bijvoorbeeld Lambda, Omega).
    2. We werken met een RS-code in F8F8 met α een wortel van X3+X+1X3+X+1. Geef de generatorveelterm van deze code.
    3. Gebruik het algoritme en de code van de vorige deelvragen om uit te rekenen wat het oorspronkelijke bericht was (ongecodeerd).
    Ontvangen bericht
    [α3,α6,1,α,α4,α4,1]
    [α3,α6,1,α,α4,α4,1]
    met rechts de constante term.

Academiejaar 2018-2019

1. (Op 3pt) In deze vraag kijken we naar het El Gamal versleutelingsprotocol. Hoe werkt het? Waarom is dit wiskundig correct? Op welke one way functie(s) is dit gebaseerd?
2. (Op 3pt)
    1. Wat is een elliptische kromme over een lichaam K? Beschrijf hoe de optelling en de (scalaire) vermenigvuldiging wordt gedefinieerd op een elliptische kromme.
    2. Wat verstaan we onder ECDLP? Beschrijf dit.
3. (Op 5pt) Toon aan dat de ternaire Golay code een perfecte 2 foutencorrigerende code is. Ter herrinnering: de ternaire Golay code heeft generatormatrix
(\|||||||| 100000010000001000000100000010000001101221112210122101121012110122\)/|||||||| (10000011111010000012210010001221000010022101000010210120000011012 2)

4. (Op 2pt) Wat is een 39-code? Als we deze bekijken als code over F3F3, waarom is deze dan niet lineair? Bestaat er een lineaire code over F2F2 met dezelfde parameters als de 39-code? Zo ja, is deze lineaire code dan equivalent met de 39-code?
5. (Op 7pt)
    1. Wat is een BCH-code? Toon aan dat er steeds een t-foutverbeterende BCH-code bestaat over FqFq. Geef ook afschattingen voor de parameters.
    2. We werken met een narrow-sense BCH-code over F3F3 die 1 fout verbeterend is, met primitief element αα als oplossing van de primitieve veelterm x3+x+1x3+x+1, met andere woorden q=2,m=3,t=1q=2,m=3,t=1. Bepaal de generatorpolynoom van deze code.
    3. Is de code uit de vorige deelvraag een perfecte code?
    4. We werken met de hierboven beschreven code en we ontvangen het bericht [1, 0, 1, 0, 1, 0, 1]. Pas het decodeeralgoritme voor BCH-codes toe en verbeter de fouten. Wat was dan de oorspronkelijke (ongecodeerde) boodschap.

Academiejaar 2017-2018

1. Waarvoor dient het index Calculus algoritme? Hoe en waarom werkt het? (3pt)
2. (4pt)
    - Beschrijf hoe de optelling en de (scalaire) vermenigvuldiging wordt gedefinieerd op een elliptische kromme
    - Beschouw over F31F31 de (discrete) elliptische kromme y2=x3+3x+12(mod31)y2=x3+3x+12(mod31). Bepaal de som van de punten P=(13,4)P=(13,4) en Q=(7,29)Q=(7,29). Bereken ook 2P2P. (Hiervoor werd de optellings- en vermenigvuldigingstabel in F31F31 gegeven op het examen.)
3. Wat zijn de 3 parameters van de ternaire Golay code. Toon dit aan en toon ook aan dat de code perfect is. (De generatormatrix van de ternaire Golay code werd gegeven op het examen (zie cursus)) (5pt)
4. Hoeveel cyclische codes over F2F2 zijn er van lengte 15? (Geef aan of je triviale codes al dan niet toelaat) (2pt)
5. (6pt)
    - Beschrijf het algoritme van Berlekamp-Massy-Forney voor RS-codes. Definieer daarbij de variabelen die je gebruikt.
    - We werken met een RS over F7F7 die 2 fouten verbeterend is, met primitief element 3 dat de vermenigvuldigingsgroep van F7F7 genereert. Bepaal de generatorpolynoom van deze code.
    - Pas het Berlekamp-Massy-Forney algoritme toe om het volgende ontvangen bericht te decoderen (gebruik de code uit vorige deelvraag)
      [4,4,3,1,5,3]
      [4,4,3,1,5,3]
      . (Interpreteer dit zo dat de laatste 3 de constante term is van de "ontvangen veelterm"). Wat was de verzonden (ongecodeerde) boodschap?

Academiejaar 2015 - 2016

1. Leg de werking van het index-calculus algoritme uit. (5pt)
2. Beschrijf kort de werking en de verschillende stappen van Rijndael. (3pt)
3. Hoe kunnen we van een cyclische code toch een systematische code maken? (2pt)
4.
    - Beschrijf het volledige algoritme om de (23,2) Golay code te decoderen.
    - Pas het in vorig puntje beschreven algoritme toe om het volgende ontvangen bericht te decoderen: [10101110001010010000000]. Wat was de verzonden (ongecodeerde) boodschap? (6pt)
5. Geef en bewijs de eigenschap die aangeeft dat je een bepaalde primitieve BCH-code met vast gekozen minimale afstand d kan construeren. Benoem hierbij de verschillende parameters die je in de formulering gebruikt. (4pt)

Academiejaar 2014 - 2015

1. Bewijs dat **Ham**(r,q)(r,q) een perfecte [qr−1q−1,qr−1q−1−r,3][qr−1q−1,qr−1q−1−r,3]-code is over FqFq.
2. Reed Solomon codes:
    - Beschrijf het algoritme van Berlekamp-Massy-Forney. Definieer hierbij je variabelen.
    - Beschouw een RS over F9F9 die 2 fouten verbeterend is, met primitief element αα dat wortel is van X2+X+2X2+X+2. Zoek de generator veelterm.
    - Geef de parameters van deze code.
    - Pas het reeds beschreven algoritme toe om het volgende bericht te decoderen
      [α2,1,α5,α4α4α5,1,α2]
      [α2,1,α5,α4α4α5,1,α2]
3. Leg de werking uit van de *baby-step giant-step* methode.
4. Bewijs of geef een tegenvoorbeeld:
    - De *EAN-13-code* is een lineaire code.
    - Bij het algoritme van het decoderen van de *extended Golay code* wordt in de eerste 6 stappen de error vector ee bepaald. De laatste stap zegt echter dat als deze vector niet bepaald is, je moet vragen de code opnieuw te verzenden. Dit algoritme wordt ook gebruikt als hulmpiddel bij het decoderen van de (perfect) **Gol**(23,2)(23,2) code. De zojuist beschreven laatste stap kan bij het decoderen van **Gol**(23,2)(23,2) niet voorkomen.

Academiejaar 2012 - 2013

1. Beschrijf de werking van het RSA-systeem, toon aan dat dit effectief werkt en leg uit welke one-wayfuncties gebruikt worden in dit systeem.
2. Bekijk de volgende binaire code CC van lengte 21 waarbij de codewoorden geschreven worden zoals in de volgende tabel:
    - x4x9x14x1x5x10x15x19x2x6x11x16x20x3x7x12x17x21x8x13x18x1x2x3x4x5x6x7x8x9x10x11x12x13x14x15x16x17x18x19x20x21
    - Toon aan dat CC een lineaire code is.
    - Wat is de dimensie van CC?
    - Wat is de minimale afstand van CC?
    - Indien de tabel
      000000001000100000000
      01000000000000000010
      ontvangen wordt, geef dan alle codewoorden die het dichtst bij dit ontvangen woord zijn.
    - Indien de tabel
      10111111011011111101
      10111111011011111101
      ontvangen wordt, geef dan alle codewoorden die het dichtst bij dit ontvangen woord zijn.
3. Ter herinnering: de extended binaire Golay code heeft generatormatrix [I12,BI12,B] (Zoek de B zelf op, ze past niet in de wiki)
    - Beschrijf het volledige algoritme om de (24,2) Golay code te decoderen.
    - Pas het voorgaande beschreven algoritme toe om het volgende ontvangen bericht te decoderen: [1 0 0 0 0 0 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 1] Wat was de verzonden (ongecodeerde) boodschap?
    - Als je een willekeurig woord van 24 bit neemt, wat is dan de kans dat je algoritme zal eindigen in een gecorrigeerd woord?
4. Stel π(X)=X4+X3+1π(X)=X4+X3+1 een primitieve veelterm van een tweefoutverbeterende binaire BCH-code (t = 2, m = 4). Bepaal de generatorveelterm van deze code, vertrekkende van een α∈F16α∈F16, wortel van deze π(X)π(X). Wat zijn de parameters van deze code?
5. Definieer wat een Reed solomon code over FqFq is en toon aan dat dit een [q-1,q-2t-1,2t+1]-code is.