Numerisk analys, MA1454 12 april 2017

Laborationsrapport

Laboration 1

Johan Almeflo, 921220-2874
Viktor Lundkvist, 920628-4912

Kryptering och steganografi medelst Newtons metod

Problemformulering

(a) I denna och uppgifterna nedan är

$$p(x) = x^5 - x^3 + 12x^2 + 36x - 2.$$

Bestäm grafiskt ett slutet intervall I för x så att ekvationen $p(x) = t$ har exakt en lösning för varje $t \in A$.

(b) Bestäm mittpunkten till I, vilken vi betecknar x_0.

(c) Implementera Newtons metod för att lösa ekvationen $p(x) = t$, där $t \in A$, dvs definiera en funktion **`kryptera(t)`** som returnerar ett flyttal $\hat{x}$ sådant att $p(\hat{x}) \approx t$. Använd x_0 som startvärde och $|x_n - x_{n-1}| \leq 10^{-15}$ som stoppkriterium.

(d) Vad döljer sig bakom följande krypterade meddelande?

`3ff5801d2444f174  3ffae1a989917c2b  3ffbe37203e3eaa5`

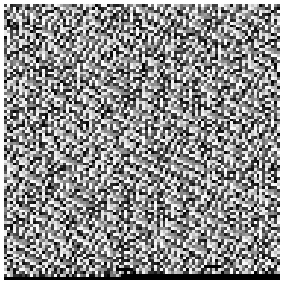
(e) Kryptera meddelandet **`Hello World!`**, där resultatet representeras hexadecimalt.

(f) Numeriska metoder är ovanliga som del av ett kryptosystem eftersom flyttalsaritmetik är alltför oprecis–alla avrundningar som görs under beräkningarna kan leda till så stora avvikelser att man vid dekryptering inte erhåller det ursprungliga meddelandet. Undersök om samtliga element i A efter kryptering dekrytperas tillbaka till samma element. Med andra ord kontrollera om

$$\lfloor p(kryptera(t)) \rceil = t$$

för alla $t \in A$ där $\lfloor x \rceil$ betecknar avrundningen av x till närmsta heltal.

(g) Man kan ”dölja” ett krypterat meddelande genom att representera det som en bild. Varje tecken $t \in A$ krypteras som sagt som ett 64 bitars flyttal, vilket i sin tur kan delas upp i åtta block om åtta bitar. Varje sådant block bestämmer gråskalan för en punkt i en punktbaserad bild, från 0 (svart) till 255 (vitt). Bilden läses rad för rad och det krävs åtta punkter för att bestämma ett flyttal. Följande bild har erhållits genom att kryptera ett meddelande med polynomet $p(x)$ ovan.



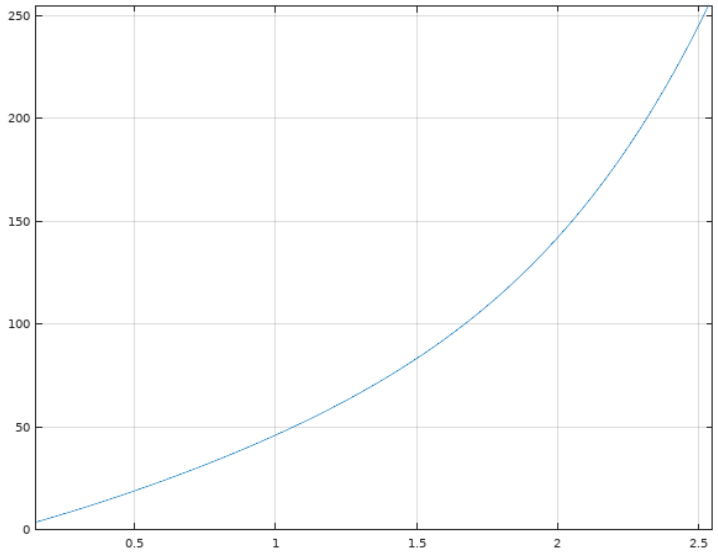
Varje element i matrisen C är ett heltal som motsvarar gråskalan för respektive bildpunkt. Bestäm meddelandet.

Lösning av problem 1

Lösning av delproblem a

Första steget var att definiera polynomet i Octave. Därefter använder vi **`fplot`** för att rita ut polynomet som en graf. Eftersom $t \in A$ är det en bra idé att begränsa y-axeln mellan 0 och 255. Utifrån den grafen vi får ut är det tydligt att ett bra intervall för x är mellan 0.15 och 2.55.

```
p = @(x) x.^5 - x.^3 + 12*(x.^2) + 36*x - 2;
fplot(p, [0.15 2.55 0 255]);
% Ritar ut grafen i intervallet: x: 0.15:2.55, y: 0:255
```



Figur 1: Grafen för polynomet $p(x)$ i deluppgift a

Svar: $I = [0.15 : 2.55]$

Lösning av delproblem b

Vårt intervall I är bestämt mellan [0.15 : 2.55] vilket ger vårt x_0 värde 1.35 eftersom det är mittpunkten.

Svar: $I = [0.15 : 2.55] \quad \Rightarrow x_0 = \frac{0.15+2.55}{2} = 1.35$

Lösning av delproblem c

I Octave skrev vi funktionen nedan för att köra Newtonws metod med inputen t på polynomet $p(x)$.

```
function f = kryptera(t)
  % Funktionen p, med dess derivata pdiff
  p = @(x) x.^5 - x.^3 + 12*(x.^2) + 36*x - 2;
  pdiff = @(x) 5*x.^4 - 3*x.^2 + 24*x + 36;
  % Mittpunkten x0
  x0 = 1.35;

  % Newtons metod för att räkna ut x
  % Sluta när |xn - xn_1| <= 10^(-15)
  xn = x0 + ((t - (p(x0)) / pdiff(x0)));
  stop = abs(xn -x0);
  while (stop > 10.^-15)
    xn_1 = xn;
    xn = xn_1 + ((t - p(xn_1)) / pdiff(xn_1));
    stop = abs(xn - xn_1);
  endwhile
  f = xn;
end
```

Svar: Se koden ovan.

Lösning av delproblem d

Vi fick fram meddelandet genom att ta hexadecimalen och konvertera det till ett nummer, för att sedan skicka in värdet till polynomet. Svaret från polynomet skickas genom char som returnerar en bokstav. Vår dekryptering gjordes enligt koden nedan.

```
% (d) Avkoda det dolda meddelandet
num = hex2num("3ff5801d2444f174");
d = p(num);
str = char(d);
num = hex2num("3ffae1a989917c2b");
d = p(num);
str = strcat(str, char(d));
num = hex2num("3ffbe37203e3eaa5");
d = p(num);
str = strcat(str, char(d));
str = ['(d) Det dolda meddelandet var: ', str];
disp(str);
```

Svar: Det krypterade meddelandet är texten ”Fel”.

Lösning av delproblem e

För att kryptera vårt meddelande gör vi om varje bokstav till en siffra med funktionen **toascii**, till exempel får ”H” värdet 72. Numret som nu representerar en bokstav skickas som input till funktionen **kryptera**. Den funktionen returnerar ett nummer som kan konverteras till ett hexdecimal värde. Vi gör sedan detta för varje tecken i vårt meddelande. Se kod nedan.

```
% (e) Kryptera meddelandet: Hello World!
message = "Hello World!";
str2 = "";
% För varje tecken, gör om det till ascii
% och sedan kryptera tecknet
for n = 1:size(message, 2);
  ascii = toascii(message(n));
  encrypted = kryptera(ascii);
  str2 = [str2, num2hex(encrypted), ' '];
end
str2 = ['(e) Det krypterade meddelandet blir: ', str2];
disp(str2);
```

Svar:

3ff5e6929fa91875	3ffae1a989917c2b	3ffbe37203e3eaa6	3ffbe37203e3eaa6
3ffc4cfc8751eca7	3fe841eac6e3b306	3ff8a7d1fee2eb66	3ffc4cfc8751eca7
3ffcb3be748e9e7c	3ffbe37203e3eaa6	3ffabb72eaf9447c	3fe8d88ef72f74fe

Lösning av delproblem f

För att undersöka detta problem gjorde vi ett kodstycke som gick igenom varje värde på $t \in A$. t krypteras och dekrypteras, därefter jämförs det nya värdet med original värdet. Stämmer det inte överens så skrivs det ut. Se kod nedan.

```
% (f) Undersök om samtliga element i A efter kryptering
% dekrypteras tillbaka till samma element
disp('(f) Element som inte matchar: ');
for i = 0:255
  i2 = round((p(kryptera(i))));
  if i != i2
    disp(i); % Skriver ut det element som inte stämmer
  end
end
```

Svar: Det fanns inga värden som skiljde sig.

Lösning av delproblem g

Först läser vi in bilden för att få ut ett gråskalevärde mellan 0 och 255 för varje pixel. Värdena grupperas upp i storlek på 8 där varje grupp konverteras ihop till ett hexadecimal värde. Därefter kan hexadecimal värdet göras om till ett nummer. Numret skickas in till vårt original polynom $p(x)$ för att returnera en siffra som med hjälp av **char** blir en läsbar bokstav. Se kod nedan.

```
% (g) Avkoda bilden
img = imread('bild-g.bmp');
imgText = "";
totalSize = size(img, 1) * size(img, 2);
rowsize = size(img, 1);
% Läs 8 tecken i taget, upp till storleken av matrisen
for i = 1:8:totalSize
  dec = [];
  for j = 0:7
    tmpValue = 0;
    % Se till så att vi inte får outofbounds
    if i + j < totalSize
      % Räkna ut vilken rad och kolumn vi är på
              % och hämta det värdet
      k = i + j - 1;
      column = floor((k / rowsize) + 1);
      row = mod(k,rowsize) + 1;
      tmpValue = img(column, row);
    end
    dec = [dec tmpValue];
  end
  % Gör om de 8 decimala tecknen till hexadecimala
  % och skriv sedan dem till en sträng, tmpText
  tmpText = '';
  hex = dec2hex(dec);
  for j = 1:size(hex,1)
    for k = 1:size(hex,2)
      tmpText = [tmpText hex(j,k)];
    end
  end
  % Avkoda vad för tecken det är och lägg sedan
  % till det till strängen imgText
  num = p(hex2num(tmpText));
  imgText = [imgText char(num)];
end
disp('(g) Bilden avkrypteras till: ');
disp(imgText);
```

Svar: Meddelandet var låttexten till sången *The Spirit of Radio*, tillsammans med en länk till youtube med ett live uppträdande av låten.

Utskrift:

The Spirit of Radio

Begin the day with a friendly voice
A companion, unobtrusive
Plays the song that's so elusive
And the magic music makes your morning mood

Off on your way, hit the open road
There is magic at your fingers
For the spirit ever lingers
Undemanding contact in your happy solitude

Invisible airwaves crackle with life
Bright antennae bristle with the energy
Emotional feedback on timeless wavelength
Bearing a gift beyond price, almost free

All this machinery making modern music
Can still be open-hearted
Not so coldly charted it's really just
A question of your honesty, yeah, your honesty

One likes to believe in the freedom of music
But glittering prizes and endless compromises
Shatter the illusion of integrity, yeah

Invisible airwaves crackle with life
Bright antennae bristle with the energy
Emotional feedback on timeless wavelength
Bearing a gift beyond price, almost free

For the words of the prophets were written on the studio wall
Concert hall
And echoes with the sound of salesmen
Of salesmen, of salesmen

https://www.youtube.com/watch?v=9RG5UV9vuxI