Secret sharing - om at dele en hemmelighed
Matematiklærerdag 2017

Johan P. Hansen

Institut for Matematik, Aarhus universitet

24. marts 2017

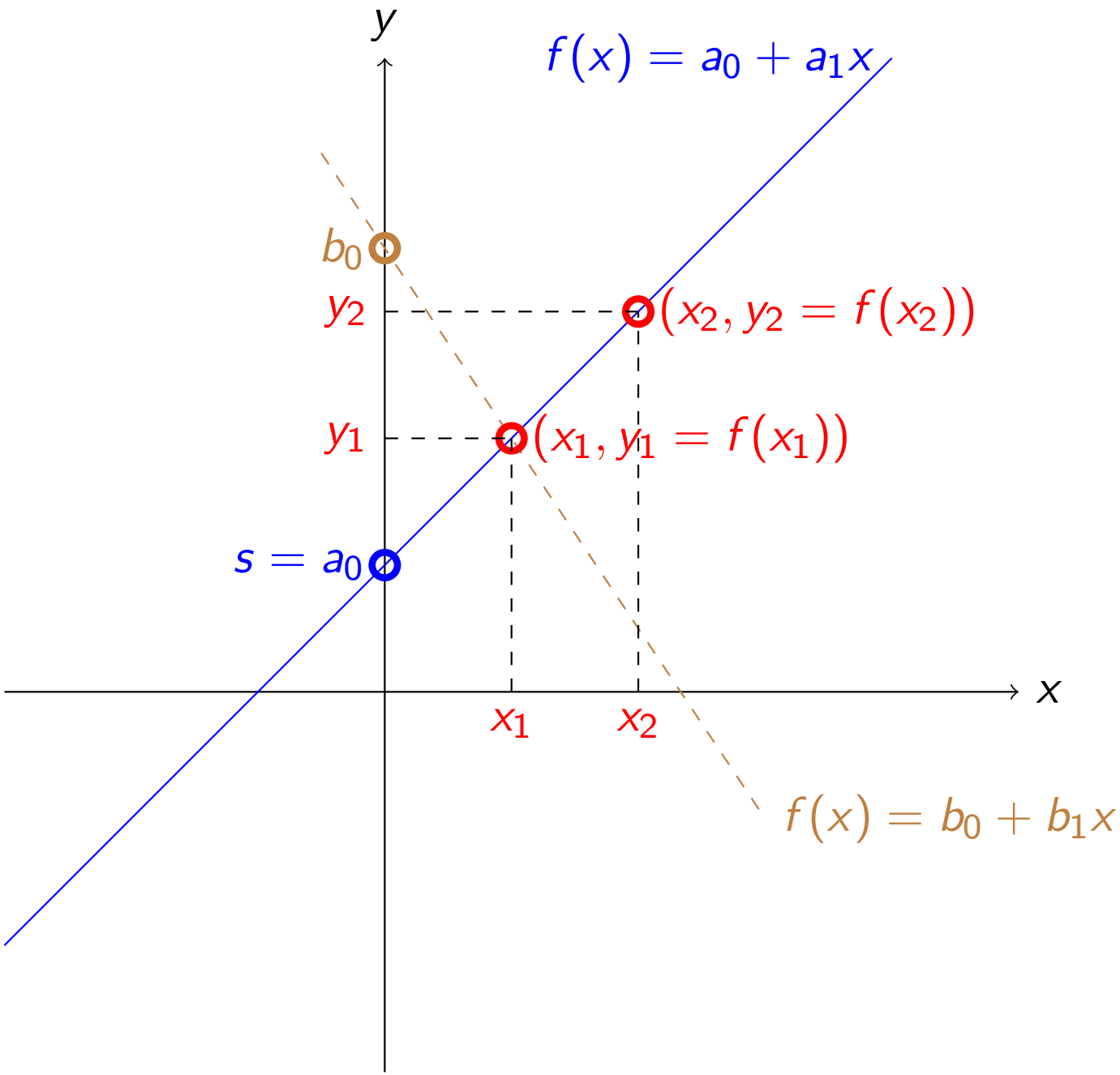
Resumé

- Secret sharing henviser til metoder til fordeling af en hemmelighed blandt en gruppe af deltagere, som hver især får tildelt en andel (et lod, en share) af hemmeligheden
- Hemmeligheden kan rekonstrueres, når et tilstrækkeligt antal af andele (lodder, shares) kombineres, hvorimod færre andele (lodder, shares) ikke giver nogen viden om hemmeligheden
- Secret sharing blev opfundet uafhængigt af Adi Shamir og George Blakley i 1979 - matematisk bygges på evaluation og interpolation af polynomier, og ville kunne behandles i gymnasieskolen

To deler en hemmelighed

To vil dele en hemmelighed s (et tal), hver part får et lod (et tal). Krav: Begge lodder skal være til stede for at afsløre hemmeligheden.

- Lad $a_0 = s$, vælg a_1 tilfældigt og lad $f(x) = a_0 + a_1 x$, hvis graf er en ret linie
- Vælg forskellige x_1, x_2 tilfældigt og evaluer $y_1 = f(x_1), y_2 = f(x_2)$ og få de 2 lodder
- Er 2 lodder kendt , er der en entydig bestemt ret linie igennem (x_1, y_1) og (x_2, y_2), hvorfor hemmelighed $s = a_0$ er bestemt
- En derimod kun 1 lod kendt, f.eks. (x_1, y_1), er der mange linier igennem dette punkt og skæringen med y-aksen b_0 kan være, hvad det skal være


y
$f(x) = a_0 + a_1 x$
b_0
y_2
$(x_2, y_2 = f(x_2))$
y_1
$(x_1, y_1 = f(x_1))$
$s = a_0$
x
x_1
x_2
$f(x) = b_0 + b_1 x$

Notation

Som altid er K er vilkårligt legeme, eksempelvis $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ eller restklasselegemet $\mathbb{Z}/p\mathbb{Z}$ (p et primtal).
Blot skal vi i K kunne addere, multiplicere og dividere (med elementer forskellige fra nul), samt regne associativt, kommutativt og med parenteser (distributivt).
At $\mathbb{Z}/p\mathbb{Z}$ (p et primtal) er et legem, se [Hansen, 2012]. Helt central er Euklids udvidede algoritme.

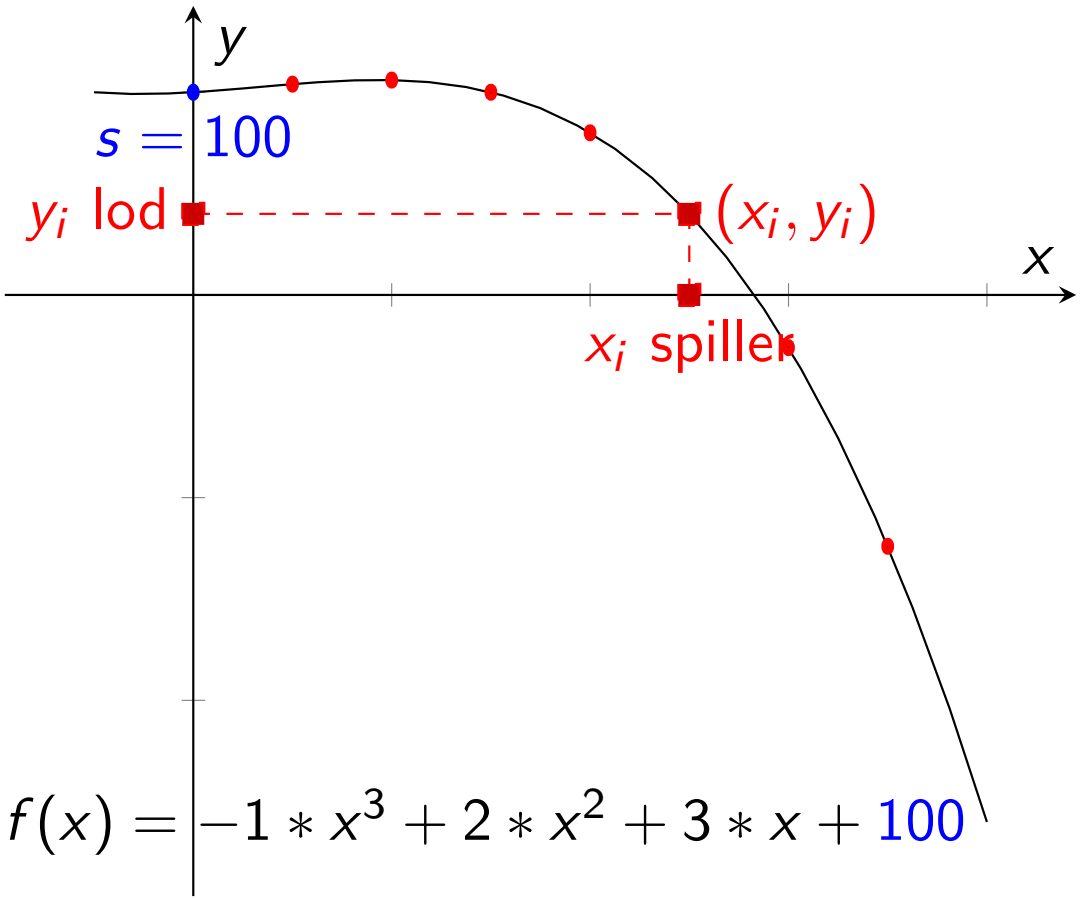
Sharmir secret sharing, se [Shamir, 1979]

En hemmelighed $s \in K$ deles i n lodder, så vilkårlige t af disse bestemmer s, hvorimod færre end t lodder ikke giver nogen viden:

- $a_0 = s$ (hemmeligheden)
- Vælg $x_1, \ldots, x_n \in K$ parvis forskellige
- Vælg tilfældige $a_1, \ldots a_{t-1} \in K$ og konstruere polynomiet

$$f(X) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$

  af grad mindre end eller lig med $t - 1$
- De n lodder er evalueringerne $y_i = f(x_i), i = 1, \ldots, n$
- Polynomiet $f(x)$ og dermed $a_0 = s$ er entydigt bestemt af vilkårlige t af evalueringerne $y_i = f(x_i), i = 1, \ldots, n$. Det er ikke tilfældet, hvis færre end t evalueringer er kendte.


y
s = 100
y_i lod
(x_i, y_i)
x
x_i spiller
$f(x) = -1 * x^3 + 2 * x^2 + 3 * x + 100$

n=7 lodder, hvoraf vilkårlige t=4 bestemmer hemmeligheden

Example

En hemmelighed $s = 100$ deles i $n = 7$ lodder, så vilkårlige $t = 4$ bestemmer $s = 100$, hvorimod færre ikke giver nogen viden:

- $a_0 = s = 100$ (hemmeligheden)
- Vælg $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4, x_5 = 5, x_6 = 6, x_7 = 7$
- Vælg (tilfældige) $a_1 = 3, a_2 = 2, a_3 = -1$ og lad

$$f(X) = 100 + 3X + 2X^2 - X^3$$

  af grad 3 (mindre end eller lig med $3 = t - 1$)
- De 7 lodder: $f(1) = 104, f(2) = 106, f(3) = 100, f(4) = 80, f(5) = 40, f(6) = -26, f(7) = -124$
- Polynomiet $f(X)$ og dermed $a_0 = s$ er entydigt bestemt af vilkårlige 4 lodder

Lagrange polynomiet

Som altid er K er vilkårligt legeme, eksempelvis $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ eller $\mathbb{Z}\backslash p\mathbb{Z}$ (p et primtal). Blot skal vi kunne addere, multiplicere og dividere (med elementer forskellige fra nul), samt regne associativt, kommutativt og med parenteser (distributivt).

Sætning

Lad $x_1, \ldots, x_t \in K$ være parvis forskellige og lad $y_1, \ldots, y_t \in K$ være vilkårlige værdier.
Der findes et entydigt bestemt polynomium $f(x)$ med koefficienter i K med $\operatorname{grad} f(x) \leq t-1$, så

$$y_i = f(x_i) \quad \text{for} \quad i = 1, \ldots, t \ . \tag{1}$$

Polynomiet kaldes Lagrange polynomiet.

Bevis.

Entydighed: Lad $f_1(x)$ og $f_2(x)$ være 2 polynomier som i (1). Dermed er

$$f_1(x_i) - f_2(x_i) = 0 \quad \text{for} \quad i = 1, \ldots, t \ .$$

Dermed har polynomiet $f_1(x) - f_2(x)$, der har grad mindre end eller lig med $t - 1$, mindst t rødder. Det er kun muligt, for nul-polynomiet, hvorfor $f_1(x)$ og $f_2(x)$ er identiske. □

Bevis.

Eksistens: Lagrange basispolynomiet

$$\ell_j(x) := \prod_{\substack{1 \le m \le t \\ m \neq j}} \frac{x - x_m}{x_j - x_m}, \quad j = 1, \ldots, t$$

har grad $t - 1$, evaluerer til 0 i $x = x_i$ $(i \neq j)$ og 1 i $x = x_j$. Polynomiet

$$L(x) := \sum_{j=1}^{t} y_j \ell_j(x)$$

har grad mindre end eller lig med $t - 1$ og evaluerer som ønsket. □

Example

De første 4 lodder i det tidligere eksempel var $f(1) = 104, f(2) = 106, f(3) = 100, f(4) = 80$.For at bestemme hemmeligheden ud fra disse, beregner vi de 4 Lagrange basispolynomier $\ell_1(x), \ell_2(x), \ell_3(x)$ og $\ell_4(x)$. Det første bliver

$$\ell_1(x) = \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} \cdot \frac{x-4}{1-4} = -\frac{1}{6}x^3 + \frac{3}{2}x^2 - \frac{13}{3}x + 4$$

Lagrange interpolationspolynomiet bliver

$$104 * \ell_1(x) + 106 * \ell_2(x) + 100 * \ell_3(x) + 80 * \ell_4(x) = \\ -x^3 + 2 * x^2 + 3 * x + 100 \ ,$$

og den delte hemmelighed er bestemt til at være 100.

Shamir Secret Sharing og Lagrange interpolation

- Kender vi t eller flere af de n lodder findes et entydigt bestemt Lagrange interpolationspolynomium af grad mindre end eller lig med $t-1$. Hemmeligheden s er bestemt
- Beviset giver en metode til at bestemme Lagrange interpolationspolynomiet
- u lodder $(u < t)$ siger **intet** om hemmeligheden s.
  Lad s_1 være en vilkårlig. Der findes et Lagrange interpolationspolynomium af grad mindre end eller lig med $u \leq t-1$ igennem de u oprindelige lodder og loddet $(0, s_1)$

Let udregning af Lagrange polynomiet - Szegö-metoden se [Szeg" o, 1975]

.

$$\pi(x) = (x - x_1)(x - x_2)\cdots(x - x_t)$$

Ved formel differentation, hvor produktreglen for differentation stadig gælder, fås

$$\frac{d}{dx}\pi(x) = \sum_{i=1}^{t}\left(\prod_{1\leq m\leq t \;\; m\neq i}(x - x_m)\right)$$

$$\pi'(x_j) = \prod_{0\leq m\leq t \;\; m\neq j}(x_j - x_m)$$

Lagrange basispolynomiet bliver

$$\ell_j(x) = \frac{\pi(x)}{(x - x_j)\pi'(x_j)}$$

SAGE - (https://cloud.sagemath.com/)

Example

SAGE - koden nedenfor bestemmer ved hjælp af Szegö-metoden udledt ovenfor Lagrange interpolationspolynomiet i vort eksempel.

```
sage: xs = [1,2,3,4]
sage: ys = [104, 106, 100, 80]
sage: pi(x) = prod(x-i for i in xs); pi(x)
sage: pid(x) = diff(pi(x),x);
sage: P(x) = sum(pi(x)/(x-i)/pid(i)*j for (i,j) in zip(xs,ys))
sage: P(x).collect(x)
```

Example

Koden nedenfor bestemmer ved hjælp af Szegö-metoden udledt ovenfor Lagrange interpolationspolynomiet i vort eksempel.

$t := 4$

$xs := 1, 2, 3, 4$

$ys := 104, 106, 100, 80$

$$\text{Define} \quad q(x) = \prod_{i=1}^{t}(x - xs[i])$$

$$qs := \text{seq}\left(\frac{d}{dx}(q(x))\middle| x = xs[i], i, 1, t\right)$$

$$\text{Define} \quad L(x) = \sum_{i=1}^{t}\left(\frac{q(x)}{(x - xs[i]) \cdot qs[i]} ys[i]\right)$$

Et polynomium af grad mindre end eller lig med $t-1$ har t koefficienter $a_i \in K$.

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$

t lodder er evalueringerne $y_i = f(x_i), i = 1, \ldots, t$ og giver anledning til t lineære ligninger i de t ubekendte koefficienter.

$$y_i = a_0 + a_1 x_i + \cdots + a_{t-1} x_i^{t-1}$$

Ligningerne kan løses da deres antal er mindre end lig med antallet af variable. Dermed kan $f(x)$ og hemmeligheden bestemmes.
Har vi kun u lodder ($u < t$), får vi u lineære ligninger, der er færre end antallet af variable, og dermed uendelig mange løsninger til ligningssystemmet.
Se f.eks. [Nielsen & Salomonsen, 2011].


Hansen, Johan P. 2012.
Tal og mængder. Begreber, metoder og resultater.
Aarhus: Aarhus Universitetsforlag.


Nielsen, Holger Andreas, & Salomonsen, Hans Anton. 2011.
Lineær algebra via eksempler.
Aarhus: Aarhus Universitetsforlag.


Shamir, Adi. 1979.
How to share a secret.
Comm. ACM, **22**(11), 612–613.


Szeg" o, Gábor. 1975.
Orthogonal polynomials. Fourth edn.
American Mathematical Society, Providence, R.I.
American Mathematical Society, Colloquium Publications, Vol. XXIII.