
Utfallsrum - Ω (en ändlig mängd).

Anta att $Pr : 2^\Omega \rightarrow \mathbb{R}$ och $p : \Omega \rightarrow \mathbb{R}$ uppfyller $0 \leq Pr(A) \leq 1$ för $A \in 2^\Omega$ och $0 \leq p(\omega) \leq 1$ för alla $\omega \in \Omega$ samt $Pr(A) = \sum_{\omega \in A} p(\omega)$ för alla $A \in 2^\Omega$ samt $Pr(\Omega) = \sum_{\omega \in \Omega} p(\omega) = 1$.

(Ω, Pr) är ett

En delmängd $A \subseteq \Omega$ är en

Med 2^Ω menas potensmängden för Ω , d.v.s. mängden av alla delmängder till Ω . Om Ω är $\Omega = \{1, 2, 3\}$ är $2^\Omega = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

X kallas här en (även). Man kan inte förutsäga värdet - det är beroende på "slumpen". Man kan ha flera stokastiska variabel per utfallsrum.

Med $X(\omega)$ menas en funktion vars värde inte är känt utan beror på "slumpen".

Skrivsätten $X \leq x$ och $X = x$ motsvarar mängderna $\{\omega \in \Omega : X(\omega) \leq x\}$ respektive $\{\omega \in \Omega : X(\omega) = x\}$.

Vidare är $p_X(x) = Pr(X = x)$ och $Pr(X \leq x) = \sum_{y \leq x} p_X(y)$.

Med A^c menas komplementet till mängden A .

Betingad sannolikhet tecknas $Pr(B|A)$.

- (a) $Pr(A) = 1 - Pr(A^c)$
- (b) $Pr(\emptyset) = 0$
- (c) $Pr(A \cup B) = Pr(A) + Pr(B) - Pr(A \cap B)$
- (d) $A \cap B = \emptyset \Rightarrow Pr(A \cup B) = Pr(A) + Pr(B)$

Tecknas $Pr(B|A)$.

Om $Pr(A) > 0$ (d.v.s $A \neq \emptyset$) så är $Pr(B|A) = \frac{Pr(A \cap B)}{Pr(A)}$.

Sannolikheten att B inträffar med förutsättningen att A inträffat.

$$Pr(B|A) = \frac{Pr(A|B)Pr(B)}{Pr(A)}$$

$$Pr(B|A) = \frac{Pr(A|B)Pr(B)}{Pr(A)} \Rightarrow$$

$$Pr(B|A)Pr(A) = Pr(A \cap B)$$

$$Pr(B|A)Pr(B) = Pr(B \cap A)$$

$$Pr(B|A)Pr(A) = Pr(A|B)Pr(B)$$

$$\Omega = \{1, 2, \dots, 35\}$$

$$A = \{1, 2, \dots, 7\}$$

$$B = \{2, 4, \dots, 34\}$$

$$Pr(A \cap B) = Pr(X \in \{2, 4, 6\})$$

$$= \sum_{x \in \{2, 4, 6\}} p_X(x)$$

$$= p(2) + p(4) + p(6)$$

$$= \frac{1}{35} + \frac{1}{35} + \frac{1}{35}$$

$$= \frac{3}{35}$$

$$Pr(B|A) = \frac{Pr(A \cap B)}{Pr(A)} = \frac{3/35}{7/35} = \frac{3}{7}$$

$$Pr(A|B) = \frac{Pr(A \cap B)}{Pr(B)} = \frac{3/35}{17/35} = \frac{3}{17}$$

$$\frac{Pr(A|B)Pr(B)}{Pr(A)} = \frac{(3/7) * (7/35)}{17/35} = \frac{3}{17}$$

När man vet den ena betingade sannolikheten kan man alltså beräkna den andra via Bayes sats.

Claude E. Shannon publicerade en serie artiklar 1948 och 1949. Lade grunden för den moderna synen på kryptering.

M är alla klartexter (så som alfabetet, alla möjliga block om åtta karakterer).

Med C menas alla kryptogram.

Alla nycklar betecknas med K .

M, C och K är stokastiska variabler som beskriver val av klartext, kryptogram och nyckel.

Vidare har vi en serie funktioner:

$$p_M(m) = Pr(M = m)$$

$$p_C(c) = Pr(C = c)$$

$$p_K(k) = Pr(K = k)$$

$$\begin{aligned} e : K \times M &\mapsto C \\ d : K \times C &\mapsto M \end{aligned}$$

Om vi samlar (M, C, K, e, d) får vi ett kryptosystem.

Vi har det svenska alfabetet, $M = C = \{a, b, \dots, ö\}$. Då är mängden möjliga nycklar $K = \{\text{alla permutationer på } (a, b, \dots, ö)\}$. Sannolikheten att ett tecken dyker upp kan exempelvis ges av $p_M(a) = 0.090$, $p_M(f) = 0.019$, $p_M(x) = 0.001$. För summan av alla dessa sannolikheter gäller $p_M(a) + p_M(b) + \dots + p_M(ö) = 1$. Sannolikheten att en viss nyckel används bestäms av $p_K(k) = \frac{1}{29!}$.

Ett kryptosystem har perfekt sekretess om $Pr(M = m | C = c) = Pr(M = m)$ för alla $m \in M$ samt alla $c \in C$. Klartexten är alltså oberoende av kryptogrammet. Det vill säga, kryptogrammet läcker ingen information om klartexten. Man kan slarvigt skriva $p(m|c) = p(m)$.

Bayes sats ger att $p(m|c)p(c) = p(c|m)p(m)$. Genom att använda detta kan vi skriva

$$\begin{aligned} p(m|c) &= p(m) \\ &\iff \\ \frac{p(c|m)p(m)}{p(c)} &= p(m) \\ &\iff \\ p(c|m) &= p(c) \end{aligned}$$

Man kan således definiera perfekt sekretess som $p(c|m) = p(c)$ - att sannolikheten att vi har ett kryptogram för en klartext är densamma som sannolikheten för att vi har ett kryptogram.

Vidare är

$$Pr(C = c | K = k) = Pr(M = d_k(c))$$

$$\begin{aligned} p(c) &= \sum_{k \in K} Pr(C = c | K = k) Pr(K = k) \\ &= \sum_{k \in K} Pr(M = d_k(c)) Pr(K = k) \end{aligned}$$

Var god se föregående exempel för monoalfabetiskt substitutionskrypto.

Med ett val av nyckel gäller:

$$Pr(C = a | K = k) = Pr(M = d_k(a) = f) = 0.019$$

Vernamchiffret (one time pad, diplomatchiffret, blankettchiffret) har perfekt sekretess.

Låt $M = \{0, 1, \dots, n - 1\} = C = K$. Krypteringsfunktionen $e(x) = x + k \pmod{n}$ och dekrypteringsfunktionen $d(x) = x - k \pmod{n}$.

För val av nyckel gäller $p(k) = \frac{1}{n}$. Det vill säga en likformig fördelning.

Vi vill visa att $p(m|c) = p(m) \iff p(c|m) = p(c)$.

För varje kryptogram c finns det en nyckel k så att $m = d_k(c)$ för alla klartexter $m \in M$. Det vill säga $M = \{d_0(c), d_1(c), \dots, d_{n-1}(c)\}$. Det betyder att $M = d_k(c)$ och $M = d_{k'}(c)$ är oberoende då $k \neq k'$. Det ger att $\sum_{k \in K} Pr(M = d_k(c)) = 1$ vilket i sin tur ger att $p(c) = \sum_{k \in K} Pr(M = d_k(c))Pr(K = k)$.

Vi har nu

$$\begin{aligned} p(c) &= \sum_{k \in K} Pr(M = d_k(c))Pr(K = k) \\ &= \sum_{k \in K} Pr(M = d_k(c))\frac{1}{n} \\ &= \frac{1}{n} \sum_{k \in K} Pr(M = d_k(c)) = \frac{1}{n} \end{aligned}$$

Frekvensanalys är alltså oanvändbart.

Vi har också att $p(c|m) = \frac{1}{n}$ eftersom för varje klartext m finns det exakt en nyckel k sådan att $c = e_k(m)$.

Det visar att $p(c) = \frac{1}{n} = p(c|m)$, vilket skulle visas.

Om ett kryptosystem har perfekt sekretess så är antal nycklar minst lika många som antalet möjliga klartexter, $|K| \geq |M|$. Om antalet nycklar är mindre än antal meddelande så har vi ej perfekt sekretess, $|K| < |M|$.

Antag att $|M| = |C| = |K|$ och att kryptosystemet har perfekt sekretess. Låt $K_{m,c} = \{k \in K : e_k(m) = c\}$. Då gäller följande:

- (a) $m \neq n \Rightarrow K_{m,c} \cap K_{n,c} = \emptyset$
- (b) $|K_{m,c}| = 1 \forall m \in M \vee c \in C$

Antag att $|M| = |C| = |K|$ och att kryptosystemet har perfekt sekretess. Låt $K_{m,c} = \{k \in K : e_k(m) = c\}$. Då gäller följande:

$$(a) p(k) = \frac{1}{|K|}$$

$$(b) |k \in K : c = e_k(m)| = 1 \quad \forall m \in M \vee c \in C$$

Man kan ställa sig frågan "hur mycket information om klartexten eller nyckeln avslöjar ett kryptogram?".

X är en stokastisk variabel (s.v.). Låt x_1, x_2, \dots, x_n vara alla utfall för X . Vidare är p_1, p_2, \dots, p_n sannolikheterna för x_k .

Entropin för X ges av $H(X) = H(p_1, p_2, \dots, p_n)$ om funktionen uppfyller tre villkor.

1. H ska vara kontinuerlig

2. $A(n) = H(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n})$ ska vara strängt växande

- $A(2) = H(\frac{1}{2}, \frac{1}{2})$

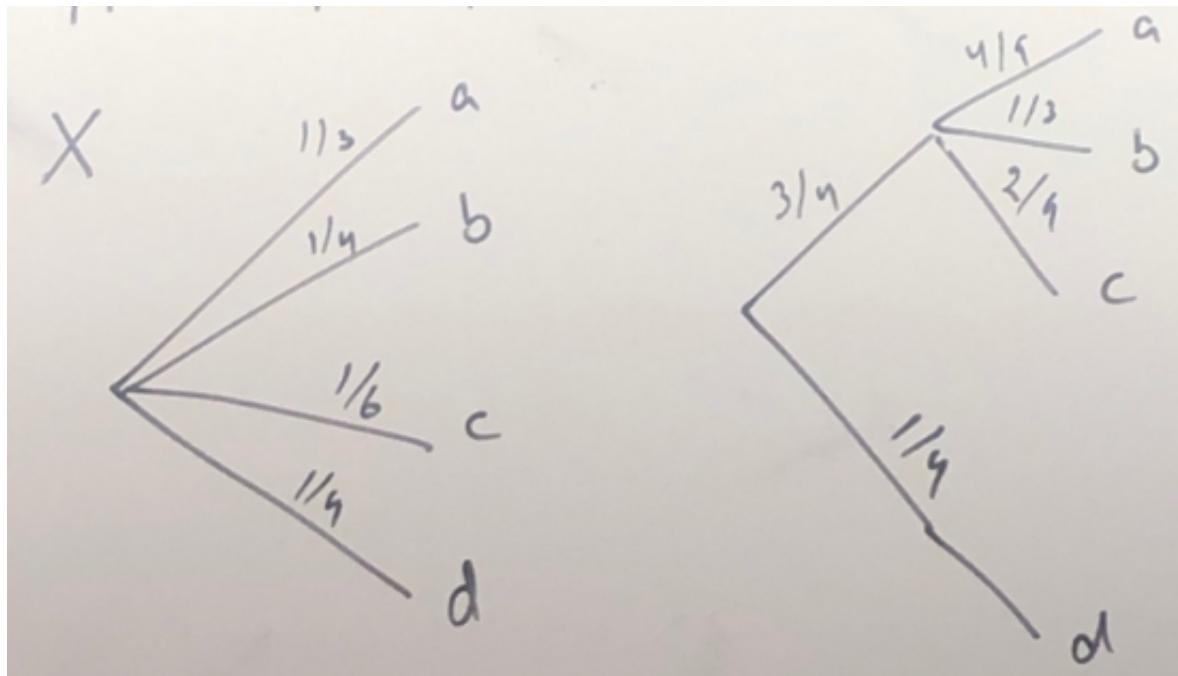
- $A(3) = H(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$

3. X är en stokastisk variabel som kan delas upp i X_1 och X_2 med sannolikheten q_1 respektive q_2 . Då är $H(X) = q_1 H(X_1) + q_2 H(X_2)$

- För X gäller $\{a, b, c, d\}$ med $p_1 = Pr(X = a) = \frac{1}{3}, p_2 = \frac{1}{4}, p_3 = \frac{1}{6}, p_4 = \frac{1}{4}$

- Om utfallen är $X_1 : \{a, b, c\}, d$ och $X_2 : a, b, c$ är $q_1 = 1$ och $q_2 = \frac{1}{3} + \frac{1}{4} + \frac{1}{6} = \frac{3}{4}$

- $H(X) = \underbrace{H(\frac{1}{3}, \frac{1}{4}, \frac{1}{6}, \frac{1}{4})}_{\text{vill}} = 1 * H(\frac{3}{4}, \frac{1}{4}) + \frac{3}{4} H(\frac{4}{9}, \frac{1}{3}, \frac{2}{9})$



Låt r vara ett positivt heltal. Då är $A(n^r) = rA(n)$.

Jämför med $\log(x^a) = a \log(x)$.

Det finns enbart en funktion som uppfyller alla tre krav för entropin ovan, nämligen:

$$H(p_1, p_2, \dots, p_n) = -K \sum_{k=1}^n p_k * \log p_k \quad K \geq 0 \quad (K = 1)$$

Om $p_k = 0$ så antas $p_k * \log p_k = 0$.

Låt m, n, s, t vara positiva heltal. Lemma ger $A(s^m) = mA(s)$ och $a(t^n) = nA(t)$. Antag att $s > 1$ och $t > 1$. Välj m så att

$$\begin{aligned} s^m &\leq t^n \leq s^{m+1} \\ &\iff m \log s \leq n \log t < (m+1) \log s \\ &\iff \frac{m}{n} \leq \frac{\log t}{\log s} \leq \frac{m}{n} + \frac{1}{n} \\ &\iff 0 \leq \frac{\log t}{\log s} - \frac{m}{n} < \frac{1}{n} \end{aligned}$$

Sätt $\epsilon = \frac{2}{n} > 0$. För stora n är ϵ litet.

$$\left| \frac{\log t}{\log s} - \frac{m}{n} \right| < \frac{\epsilon}{2}$$

För kravet $A(n)$ är strängt växande får vi

$$\begin{aligned} A(s^m) &\leq A(t^n) < A(s^{m+1}) \\ &\iff mA(s) \leq nA(t) < (m+1)A(s) \\ &\iff \frac{m}{n} \leq \frac{A(t)}{A(s)} < \frac{m}{n} + \frac{1}{n} \\ &\iff \left| \frac{A(t)}{A(s)} - \frac{m}{n} \right| \end{aligned}$$

Triangelolikheten $|x+y| \leq |x| + |y|$ ger oss

$$\begin{aligned} \left| \frac{A(t)}{A(s)} - \frac{\log t}{\log s} \right| &= \left| \frac{A(t)}{A(s)} - \frac{m}{n} + \frac{m}{n} - \frac{\log t}{\log s} \right| \\ &\leq \left| \frac{A(t)}{A(s)} - \frac{m}{n} \right| + \left| \frac{m}{n} - \frac{\log t}{\log s} \right| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{aligned}$$

Parantes: eftersom d ej beror på n medan ϵ gör det och att vi kan göra ϵ hur litet som helst, måste $d = 0$. Alltså är

$$\frac{A(t)}{A(s)} = \frac{\log t}{\log s}$$

Håll s konstant och sätt $K = \frac{A(s)}{\log s}$. Då är

$$\begin{aligned} \left| \frac{A(t)}{A(s)} - \frac{\log t}{\log s} \right| &< \epsilon \\ \iff \underbrace{\left| \frac{1}{A(s)} \right| * \left| A(t) - \underbrace{\frac{A(s)}{\log s}}_K * \log t \right|} &< \epsilon \\ \iff L |A(t) - K \log t| &< \epsilon \end{aligned}$$

För stora m är ϵ litet, men olikheten uppfylls (t beror ej på n). Alltså är

$$A(t) = K \log t$$

Låt X vara en stokastisk variabel med n olika utfall med sannolikheterna p_1, p_2, \dots, p_n där $p_i = \frac{m_i}{m}$ och $m = m_1 + m_2 + \dots + m_n$.

Låt Y vara en stokastisk variabel för likformig sannolikhet bland de m utfallen.

$$\begin{aligned} H(Y) &= H(p_1, p_2, \dots, p_n) + \sum_{i=1}^n p_i H\left(\frac{1}{m_i}, \frac{1}{m_i}, \dots, \frac{1}{m_i}\right) \\ &= H(x) + \sum_{i=1}^n p_i A(m_i) = H(x) + \sum_{i=1}^n p_i K \log m_i \end{aligned}$$

Det ger att

$$\begin{aligned} \sum_{i=1}^n p_i K \log m &= H(X) + \sum_{i=1}^n p_i K \log m_i \\ \iff H(x) &= \sum_{i=1}^n (p_i K \log m - p_i K \log m_i) \\ \iff &- \sum_{i=1}^n p_i K \log \frac{m_i}{m} \\ &= -K \sum_{i=1}^n p_i \log p_i \end{aligned}$$

på engelska.

Låt V vara en icke-tom mängd och definiera skalärmultiplikation och addition så att $au \in V$ och $u + v \in V$ där $a \in \mathbb{F}$ (\mathbb{F} är en kropp) och $u, v \in V$. Om följande uppfylls för alla $u, v, w \in V$ och alla $a, b \in \mathbb{F}$, så får vi kalla V för ett vektorrum. Det vill säga, kraven på ett vektorrum är följande:

- (a) $u + v = v + u$
- (b) $u + (v + w) = (u + v) + w$
- (c) $a(bu) = (ab)u$
- (d) $1 * u = u$
- (e) $\exists \emptyset \in V : u + \emptyset = \emptyset + u = u$
- (f) $(a + b)u = au + bu$
- (g) $a(u + v) = au + av$
- (h) $\forall u \in V \exists u' \in V : u + u' = u' + u = \emptyset$

$\emptyset \in V$ är entydigt bestämd.

Antag att \emptyset_1 och \emptyset_2 uppfyller (e). Då är

$$\emptyset_1 = \emptyset_1 + \emptyset_2 = \emptyset_2$$

- Varje vektorrum, utom nollrummet $\{\emptyset\}$ har en bas
- Varje bas till ett vektorrum har lika många vektorer

Låt $v_1, v_2, \dots, v_m \in V$. Då är en

$a_1v_1 + a_2 + v_2 + \dots + a_mv_m$ där

$a_1, a_2, \dots, a_m \in \mathbb{F}$.

om $a_1v_1 + \dots + a_mv_m = 0$ endast har $a_1 = a_2 = \dots = a_m = 0$ som lösning.

v_1, v_2, \dots, v_m är en för V om de är linjärt oberoende och om alla $v \in V$ kan skrivas som $v = a_1v_1 + a_2v_2 + \dots + a_mv_m$.

Låt $u, v \in V$. av u och v betecknas $\langle u, v \rangle$ som är en skalär, det vill säga tillhör \mathbb{F} . Följande ska vara uppfyllt:

- (a) $\langle u, u \rangle \in \mathbb{R}$
- (b) $\langle u, u \rangle \geq 0, u = 0 \iff \langle u, u \rangle = 0$
- (c) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
- (d) $\langle au, v \rangle = a\langle u, v \rangle$
- (e) $\langle u, v \rangle = \langle v, u \rangle$

Normalen, $\|u\| = \sqrt{\langle u, u \rangle} = \sqrt{x_1^2 + x_2^2 + \dots + x_n^2}$.

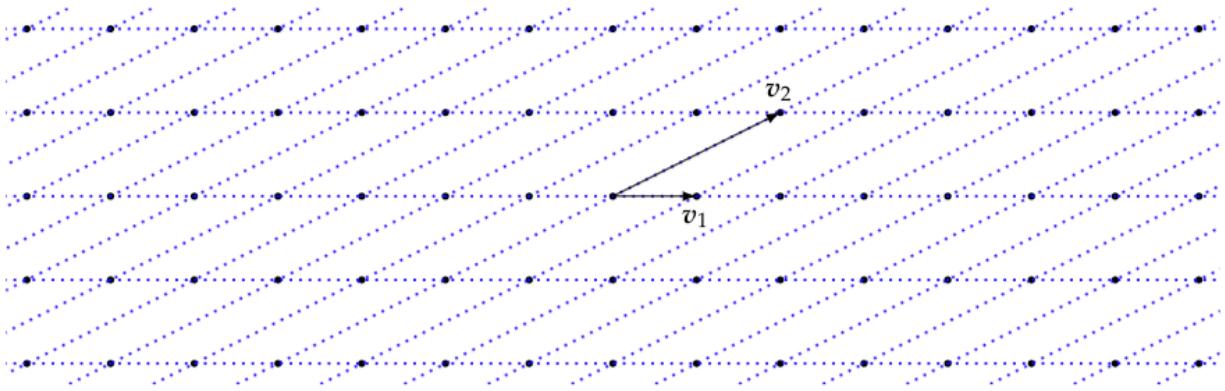
$$\langle u, v \rangle = \langle (x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \rangle = \\ x_1 y_1 + x_2 y_2 + \dots + x_n y_n$$

Låt $m \geq n$ och låt v_1, v_2, \dots, v_n vara linjärt oberoende vektorer i \mathbb{R}^m . Då kallas följande mängd för ett :

$$L = L(v_1, v_2, \dots, v_n) \\ = \{a_1 v_1 + a_2 v_2 + \dots + a_n v_n : a_k \in \mathbb{Z}\}$$

Vi kommer bara åt vissa punkter. Se bilden nedan.

Låt $v_1 = (1, 0)$ och $v_2 = (2, 1)$ i \mathbb{R}^2 .



$$L = L(v_1, v_2) \\ = \{a_1 v_1 + a_2 v_2 : a_1, a_2 \in \mathbb{Z}\} \\ = \{a_1(1, 0) + a_2(2, 1) : a_1, a_2 \in \mathbb{Z}\} \\ = \{(a_1 + 2a_2, a_2) : a_1, a_2 \in \mathbb{Z}\}$$

Även $w_1 = (3, 2)$ och $w_2 = (1, 1)$ är en bas för L ty $w_1 = -v_1 + 2v_2$ och $w_2 = -v_1 + v_2$ (samtidigt). Basbytesmatrisen ges då av

$$A = \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}$$

Vidare är $\det(A) = (-1) * 1 - 2(-1) = 1$.

Mängden $\mathcal{F} = \mathcal{F}(v_1, v_2, \dots, v_n) = \{t_1 v_1 + t_2 v_2 + \dots + t_n v_n : 0 \leq t_k \leq 1\}$ kallas för för L med avseende på v_1, v_2, \dots, v_n .

Sambandet mellan två baser för ett gitter ges av en basbytesmatris A med heltalselement. Vidare gäller att determinanten $\det(A) = \pm 1$.

Låt L vara ett gitter av dimension n och \mathcal{F} dess fundamentala parallelepiped. Då kan varje $w \in \mathbb{R}^n$ skrivas på formeln $w = t + v$ där $t \in \mathcal{F}$ och $v \in L$ på ett entydigt sätt.

Det finns två problem som används för kryptering med gitter. Dessa är främst svåra att lösa i höga dimensioner.

Finn en vektor v i $L \setminus \{\emptyset\}$ som minimerar $\|v\|$.

Givet en vektor $w \in \mathbb{R}^m \setminus L$ finn den vektor $v \in L$ som minimerar $\|v - w\|$.

Låt $v_i = (r_{i,1}, r_{i,2}, \dots, r_{i,n})$, $i = 1, 2, \dots, n$.

$$F = \begin{pmatrix} r_{1,1} & r_{1,1} & \dots & r_{1,n} \\ r_{2,1} & r_{1,1} & \dots & r_{1,n} \\ \dots & \dots & \dots & \dots \\ r_{n,1} & r_{n,1} & \dots & r_{n,n} \end{pmatrix}$$

Vidare är volymen $\text{vol } F = |\det F|$.

I två dimensioner är detta alltså samma sak som arean.

Finn en bas v_1, v_2, \dots, v_n för L så att $\max(\|v_1\|, \|v_2\|, \dots, \|v_n\|)$ eller $\|v_1\| + \|v_2\| + \dots + \|v_n\|$ är så liten som möjlig.

Minimera v så att

$$\|v\| \leq \psi(n) * \|v_{\text{shortest}}\|, \quad v \in L$$

Med v_{shortest} menas resultatet från SVP.

Minimera v så att

$$\|w - v\| \leq \psi(n) \|v_{\text{closest}} - w\|$$

med v_{closest} menas resultatet från CVP.

Varje gitter L med dimensionen n innehåller en vektor $v \neq 0$ sådan att $\|v\| \leq \sqrt{n}(\det L)^{1/n}$ där $\det L$ är $\det(v_1 \ v_2 \ \dots \ v_n)$.

för basen $B = (v_1, v_2, \dots, v_n)$ ges av $\mathcal{H} = \left(\frac{\det L}{\|v_1\| * \|v_2\| * \dots * \|v_n\|} \right)^{1/n}$.

$$0 \leq \mathcal{H}(B) \leq 1$$

Ju närmare $\mathcal{H}(B)$ är 1 desto mer ortogonal är basen B .

Låt S vara en delmängd till \mathbb{R}^n .

Om $\|v\| < r \forall v \in S, r$ konstant så säges S vara c .

Om $-v \in S$ då $v \in S$ så säges S vara r .

Om varje vektor på linjesegmentet mellan u och v där $u, v \in S$ också tillhör S så säges S vara r .

Låt $c \in S$ och $r > 0$. Den c

r ges av

$$B_r(c) = \{v \in \mathbb{R}^n : \|c - v\| \leq r\}.$$

S är c om det för varje $c \in \mathbb{R}^n$ gäller att om $B_r(c) \cap S \neq \emptyset$ för alla $r > 0$, så $c \in S$.

L är ett gitter av dimension n . $S \subset \mathbb{R}^n$ där S är symmetriskt som uppfyller

$$\text{vol}(S) > 2^n \det L$$

då finns det $v \in L \setminus \{0\}$ som tillhör S .

Låt $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ vara våra basvektorer. Vi vill minimera $\|v\|$ där $v \neq 0$. Om basen är ortogonal, dvs. $\langle v_i, v_j \rangle = 0$ då $i \neq j$. Då är

$$\begin{aligned} \|v\|^2 &= \langle v, v \rangle \\ &= \langle a_1 v_1 + \dots + a_n v_n, a_1 v_1 + \dots + a_n v_n \rangle \\ &= \langle a_1 v_1, a_1 v_1 + \dots + a_n v_n \rangle \\ &\quad + \langle a_2 v_2 + \dots + a_n v_n, a_1 v_1 + \dots + a_n v_n \rangle \\ &= \dots \\ &= a_1^2 \langle v_1, v_1 \rangle + \dots + a_n^2 \langle v_n, v_n \rangle \\ &= a_1^2 \|v_1\|^2 + a_2^2 \|v_2\|^2 + \dots + a_n^2 \|v_n\|^2 \end{aligned}$$

Om v_k är den kortaste basvektorn sätter vi $a_k = 1$ och övriga $a_i = 0$.

Låt $x \in \mathbb{R}$. Då betecknar $\lfloor x \rfloor$ det närmaste heltalat till x . Exempelvis är $\lfloor 1.2 \rfloor = 1$, $\lfloor 3.5 \rfloor = 4$.

Låt $L = L(v_1, v_2, \dots, v_n)$ vara gitter $w \in \mathbb{R}^n \setminus L$. Om $B = (v_1, v_2, \dots, v_n)$ är tillräckligt ortogonal så löser följande algoritm CVP.

1. Bestäm $t_1, t_2, \dots, t_n \in \mathbb{R}$ så att $w = t_1 v_1 + t_2 v_2 + \dots + t_n v_n$
2. Sätt $a_i \leftarrow \lfloor t_i \rfloor$ där $i = 1, 2, \dots, n$
3. Returnera $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$

$$v_1 = (2, 1), v_2 = (-1, 3)$$

$$\det L = \det \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} = 7$$

$$\|v_1\| = \sqrt{5}$$

$$\|v_2\| = \sqrt{10}$$

$$\mathcal{H}(B) = \left(\frac{\det L}{\|v_1\| * \|v_2\|} \right)^{1/2} = \sqrt{\frac{7}{5\sqrt{2}}} \approx 0.9949$$

Vi ser att B är väldigt nära att vara ortogonal.

$$w = (17, 21) = t_1 v_1 + t_2 v_2 = \frac{72}{2} v_1 + \frac{25}{7} v_2 \notin L$$

$$a_1 = \lfloor t_1 \rfloor = 10$$

$$a_2 = \lfloor t_2 \rfloor = 4$$

Närmsta vektorn i L till w är

$$v = a_1 v_1 + a_2 v_2 = 10(2, 1) + 4(-1, 3) = (16, 22)$$

Ett asymmetriskt kryptosystem från 1997 av Oded Goldreich, Shafi Goldwasser, Shai Halevi.

Går att knäcka. Kryptogrammet läcker information om klartexten.

Låt n vara ett positivt heltal. Därefter välj n linjärt oberoende vektorer $v_1, v_2, \dots, v_n \in \mathbb{Z}^n$ och $\mathcal{H}(v_1, v_2, \dots, v_n)$ nära 1. Välj sedan en $n \times n$ -matris $U = (u_{i,j})$ med heltalselement och sådan att $\det U = \pm 1$.

$$V = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, W = UV$$

Notera att om

$$W = V = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

så är

$$\begin{cases} w_1 &= u_{1,1}v_1 + u_{1,2}v_2 + \dots + u_{1,n}v_n \\ w_2 &= u_{2,1}v_1 + u_{2,2}v_2 + \dots + u_{2,n}v_n \\ \vdots & \\ w_n &= u_{n,1}v_1 + u_{n,2}v_2 + \dots + u_{n,n}v_n \end{cases}$$

Vi har att $L(v_1, v_2, \dots, v_n) = L(w_1, w_2, \dots, w_n)$ och kravet $\mathcal{H}(w_1, w_2, \dots, w_n)$ ska vara nära 0.

: w_1, w_2, \dots, w_n

: v_1, v_2, \dots, v_n

Ett meddelande kodas som en vektor

$$m = (m_1, m_2, \dots, m_n) \in \mathbb{Z}^n$$

så att $\|m\| \leq N$. Välj en efemär nyckel $r \in \mathbb{Z}^n \setminus L$.

Kryptogrammet $e \in \mathbb{Z}^n$ ges av

$$e = mW + r$$

Notera att mW finns i gittret men att $mW + r$ lämnar gittret. Kan ses som en störning. Eve behöver lösa ett CVP.

Bestäm t_1, t_2, \dots, t_n så att $e = t_1v_1 + t_2v_2 + \dots + t_nv_n$. Notera att talen ej kommer att vara heltal. Därför kan vi utnyttja Babais algoritm för att få $v = \lfloor t_1 \rfloor v_1 + \lfloor t_2 \rfloor v_2 + \dots + \lfloor t_n \rfloor v_n$. Det ger att $v = mW$, vi har alltså "trollat bort" störningen r och vi är nu återigen inom gittret. Vi har löst CVP. Klartexten kan nu fås med $m = vW^{-1}$.

$$v_1 = (5, 1, -3)$$

$$v_2 = (1, -2, 6)$$

$$v_3 = (-3, 7, 1)$$

$$\mathcal{H}(v_1, v_2, v_3) \approx 0.94$$

$$V = \begin{pmatrix} 5 & 1 & -3 \\ 1 & -2 & 6 \\ -3 & 7 & 1 \end{pmatrix}$$

$$U = \begin{pmatrix} 42 & 9 & 52 \\ 45 & -5 & 63 \\ -1 & 66 & 102 \end{pmatrix}$$

$$\det U = 1$$

$$W = UV = \begin{pmatrix} 45 & 424 & -128 \\ 31 & 496 & -102 \\ -245 & 581 & 501 \end{pmatrix}$$

$$\mathcal{H}(w_1, w_2, w_3) \approx 0.01$$

$$m = (17, 3, 11)$$

$$r = (2, -1, 1)$$

$$e = mW + r = (-1835, 15086, 3030)$$

$$e = \frac{101432}{121}v_1 + \frac{67557}{121}v_2 + \frac{24144}{11}v_3$$

$\lfloor \odot \rfloor \Rightarrow$

$$v = 838v_1 + 558v_2 + 2195v_3$$

$$vW^{-1} = (838 \ 558 \ 2195) \frac{1}{242} \begin{pmatrix} -307758 & 286792 & \dots \\ \vdots & \ddots & \dots \\ \dots & \dots & -9176 \end{pmatrix} = (17, 3, 11)$$

Om Eve gör samma sak fast då $v \leftarrow w$ får hon

$$e = a_1w_1 + a_2w_2 + a_3w_3$$

$$v = (-1746, 14216, 285\dots)$$

$$m' = (-3064, 2874, -192)$$

Detta då Eve får en "dålig bas".

Exempel på ringar \mathbb{Z} , \mathbb{Z}_m , där m är sammansatt.

Typiskt för ringar: division fungerar inte alltid.

Låt R vara en ring. Då betecknar $R[x]$ mängden av alla polynom med koefficienter ur R .

: $R[X]$ är en ring.

Om $f(x) - g(x) = m(x)n(x)$ för något polynom $n(x)$, då skriver vi att $f(x) \equiv g(x) \pmod{m(x)}$

Låt N vara ett positivt heltal och sätt

$$\begin{aligned} R &= \mathbb{Z}[x]/(x^N - 1) \\ &= \{a_{N-1}x^{N-1} + \dots + a_2x^2 + a_1x + a_0 : a_k \in \mathbb{Z}\} \end{aligned}$$

Det vill säga alla möjliga rester vi kan få när vi delar med $(x^N - 1)$.

Låt $f, g \in R$. Det vill säga $f(x) = \sum_{i=0}^{N-1} a_i x^i$ och $g(x) = \sum_{i=0}^{N-1} b_i x^i$. Då motsvaras fg av faltningen $f(x) * g(x) = (f * g)(x) = \sum_{k=0}^{N-1} c_k x^k$ där $c_k = \sum_{i+j=k \pmod{N}} a_i b_j$. Notera att "stjärnan" skrivs som just det.

Låt $N = 4$, $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ och $g(x) = b_3x^3 + b_2x^2 + b_1x + b_0$.

$$\begin{aligned} f(x) * g(x) &= c_3x^3 + c_2x^2 + c_1x + c_0 \\ c_0 &= a_0b_0 + a_1b_3 + a_2b_2 + a_3b_1 \\ c_1 &= a_0b_1 + a_1b_0 + a_2b_3 + a_3b_2 \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 + a_3b_3 \\ c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \end{aligned}$$

Låt q vara ett heltal större än 1. Sätt $R_q = \mathbb{Z}_q[x]/(x^N - 1)$.

Låt $f(x) = \sum_{i=0}^{N-1} a_i x^i \in R$.

Sätt $a'_i \equiv a_i \pmod{q}$ så att $a'_i \in \mathbb{Z}_q$ och sätt $f_q(x) = \sum_{i=0}^{N-1} a'_i x^i$ (reducering).

Givet $f_q(x) = \bar{a}_{N-1}x^{N-1} + \dots + \bar{a}_2x^2 + \bar{a}_1x + \bar{a}_0 \in R_q$. Vi vill bestämma $f \in R$ så att f reducerar f_q (alltid samma f för aktuellt f_q).

Sätt $a_k \equiv \bar{a}_k \pmod{q}$ där $\frac{-q}{2} < a_k \leq \frac{q}{2}$.

$$\begin{aligned} f_{11}(x) &= 9x^4 + 7x^2 + x + 5 \\ f(x) &= -2x^4 - 4x^2 + x + 5 \end{aligned}$$

-th degree cated polynmoial ring.

Låt N vara ett heltal större än 1. Låt d_1 och d_2 vara icke-negativa heltal. $\tau(d_1, d_2)$ är mängden av alla polynom ur R så att exakt d_1 stycken av koefficienterna är 1 och exakt d_2 stycken är -1 samt resten 0.

$$: x^5 - x^4 + x^2 - x + 1 \in \tau(3, 2).$$

Välj N och p primtal samt ett positiva heltal q och d så att $\gcd(N, p) = 1$ och $\gcd(p, q) = 1$ och $q > (6d + 1)p$. Välj $f(x) \in \tau(d + 1, d)$ och $g(x) \in \tau(d, d)$.

Reduktion: $f_p(x)$ och $f_q(x)$.

Sätt $h_q(x) = f_q^{-1}(x) * g_q(x)$ där $f_q(x) * f_q^{-1} = 1$ ty f måste väljas så.

Publika parametrar: N, p och q . Publik nyckel: h_q . Privat nyckel är f och g .

Välj en klartext som kodas som ett polynom $m_p(x) \in R_p$.

Centrerad lyftning $m(x) = \text{centrerad lyftning}(m_p(x))$.

Välj en (slumpmässig) efemär nyckel $r(x) \in \tau(d, d)$.

Kryptogrammet ges av $e(x) = ph_q(x) * r(x) + m(x)$ (reduktion). Notera att $*$ är faltningsoperatorn.

Bestäm polynomet $\bar{a}(x) = f_q(x) * e(x) \in R_q$ där $*$ innebär faltning. Gör en lyftning $a(x) = \text{centrerad lyftning}(\bar{a}(x))$. Bestäm $b(x) = f_p^{-1}(x) * a(x) \in R_p$.

Meddelandet ges av $m_p(x) = b(x)$.

Samtliga $*$ innebär här faltning.

$$\begin{aligned} N &= 7, \quad p = 5, \quad q = 71, \quad d = 2 \\ f(x) &= x^6 + x^5 - x^3 - x + 1 \in \tau(3, 2) \\ g(x) &= x^4 - x^3 + x - 1 \in \tau(2, 2) \\ f_5^{-1}, \quad f_{71}^{-1} &\text{ existerar} \\ f_5^{-1}(x) &= x^4 + 3x^3 + 4x^2 + 3x \\ f_{71}^{-1}(x) &= 46x^6 + 50x^5 + 43x^4 - 56x^3 + 30x^2 + 12x + 48 \\ h_{71}(x) &= f_{71}^{-1} * g_{71}(x) = 49x^6 + 46x^5 + 49x^4 + 43x^3 + 57x^2 + 29x + 11 \\ m_5(x) &= 4x^5 + 2x^4 + 2x^3 + 3x + 3 \\ m(x) &= \text{central lyftning}(m_5(x)) = -x^5 + 2x^4 + 2x^3 - 2x - 2 \\ r(x) &= x^6 - x^3 + x^2 - 1 \\ e(x) &= 53x^6 + 15x^5 + 56x^4 + 51x^3 + 24x^2 + 11x + 2 \end{aligned}$$

Vi har en publik nyckeln $h(x) = h_0 + h_1x + h_2x^2 + \dots + h_{N-1}x^{N-1}$ och en privat nyckel $f \in \tau(d+1, d)$.

Representation som vektor: $\bar{h} = (h_0, h_1, h_2, \dots, h_{N-1}) \in \mathbb{Z}^N$.

Rotation: $x^i * h(x) = h_{N-i} + h_{N-i-1}x + \dots + h_0x^{N-i}$ där $*$ är faltning. Exempel då $i = 1$: $x * h(x) = h_{N-1} + h_0x + h_1x^2 + h_2x^3 + \dots + h_{N-2}x^{N-1}$.

Vi bildar följande matris:

$$H = \begin{pmatrix} h \\ x * h \\ x^2 * h \\ \vdots \\ x^{N-1} * h \end{pmatrix} = \begin{pmatrix} h_0 & h_1 & h_2 & \dots & h_{N-1} \\ h_{N-1} & h_0 & h_1 & \dots & h_{N-2} \\ h_{N-2} & h_{N-1} & h_0 & \dots & h_{N-3} \\ \vdots & & & & \\ h_1 & h_2 & h_3 & \dots & h_0 \end{pmatrix}$$

Sätt $\bar{f} = (f_0, f_1, \dots, f_{N-1})$ och $\bar{g} = (g_0, g_1, \dots, g_{N-1})$.

Notera: På labben när vi "knäcker" NTRU kan det vara så att vi måste utföra en rotation för att få fram rätt. Man kan få fram olika kandidater där inte alla fungerar, så man bör därför testa mot klartexten.

Vidare sätt

$$M_h^{\text{NTRU}} = \begin{pmatrix} I & H \\ 0 & qI \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & h_0 & h_1 & h_2 & \dots & h_{N-1} \\ 0 & 1 & 0 & \dots & 0 & h_{N-1} & h_0 & h_1 & \dots & h_{N-2} \\ 0 & 0 & 1 & \dots & 0 & h_{N-2} & h_{N-1} & h_0 & \dots & h_{N-3} \\ & & & & & \dots & \dots & & & \\ 0 & 0 & 0 & \dots & 1 & h_1 & h_2 & h_3 & \dots & h_0 \\ 0 & 0 & 0 & \dots & 0 & q & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & q & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & q & \dots & 0 \\ & & & & & \dots & \dots & & & \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & q \end{pmatrix}$$

Vidare har vi att $\det M_h^{\text{NTRU}} q^N = q \neq 0$. Det vill säga att raderna i matrisen är linjärt oberoende. Vi kan alltså använda raderna för att generera ett gitter som är kopplat till detta krypto.

Låt L_h^{NTRU} vara det gitter som genereras av raderna i M_h^{NTRU} .

Låt $\bar{u} = (u_1, u_2, \dots, u_N)$ och $\bar{v} = (v_1, v_2, \dots, v_N)$. Med skrivsättet (\bar{u}, \bar{v}) så menas vektorn $u_1, u_2, \dots, u_N, v-1, v_2, \dots, v_N \in \mathbb{Z}^2$.

Låt $f, g, h \in R_q = \mathbb{Q}[x]/(x^N - 1)$. Antag att $f(x) * h(x) \equiv g(x) \pmod{q}$. Då gäller att $(\bar{f}, -\bar{u}) M_h^{\text{NTRU}} = (\bar{f}, \bar{g})$ där $f(x) * h(x) = g(x) + qu(x)$. Alltså gäller $(\bar{f}, \bar{g}) \in L_h^{\text{NTRU}}$.

Det vill säga det finns i gittret.

Givet v_1, v_2, \dots, v_n linjärt oberoende vektorer, men ej parvist ortogonalala så vill vi bestämma w_1, w_2, \dots, w_n som är linjärt oberoende och parvis ortogonalala så att v_1 och w_1 spänner upp samma underum. Detta gäller för v_1, v_2 och w_1, w_2, v_1, v_2, v_3 och w_1, w_2, w_3 o.s.v.

$$\begin{aligned}
 w_1 &\leftarrow v_1 \\
 \forall i \in \{2, 3, \dots, n\} : \\
 \mu_{i,j} &\leftarrow \frac{\langle v_i, w_j \rangle}{\|w_j\|^2}, j = 1, 2, \dots, i-1 \\
 w_i &\leftarrow v_i - \mu_{i,1}w_1 - \mu_{i,2}w_2 - \dots - \mu_{i,i-1}w_{i-1}
 \end{aligned}$$

Låt $B = (v_1, v_2, \dots, v_n)$ vara en bas som genererar ett gitter L och låt $B^* = (w_1, w_2, \dots, w_n)$ vara motsvarande bas efter att vi applicerat GSop.

Man säger att B är om radvektorerna i B uppfyller följande två olikheter: $|\mu_{i,j}| \leq \frac{1}{2}$ och $\|w_i\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|w_{i-1}\|^2$ för alla i och j . Den sistnämnda kallas Lovász olikhet.

En LLL-reducerad bas är en bra bas, det vill säga $\mathcal{H}(B)$ är nära 1.

Givet $B = (v_1, v_2, \dots, v_n)$ bas för L .

1. $k \leftarrow 2$
2. för $j = k-1, \dots, 2, 1$
 1. $v_k \leftarrow v_k - \lfloor \mu_{k,j} \rfloor v_j$
 3. om $\|w_k\|^2 \geq (\frac{3}{4} - \mu_{k,k-1}^2)\|w_{k-1}\|^2$
 1. $k \leftarrow k+1$ och gå till steg 5
 4. Byt plats på vektorerna v_{k-1} och v_k och sätt $k \leftarrow \max(k-1, 2)$
 5. Avbryt om $k > n$, annars gå till steg 2

Så fort någon vektor v_k ändras måste de $\mu_{i,j}$ och w_j som berörs bestämmas på nytt med GSop.

Använts för att analysera symmetriska krypton. Känd klartext-attack. Togs fram av Mitsuru och Matsui 1993.

Med \oplus menas vidare addition i \mathbb{Z}_2 .

Indata: $x = (x_1, x_2, \dots)$, $x_i \in \mathbb{Z}_2$. Utdata: $y = (y_1, y_2, \dots)$, $y_i \in \mathbb{Z}_2$.

Vi vill hitta någon form av linjärapproximation $x_{i1} \oplus x_{i2} \oplus \dots \oplus x_{ir} \oplus y_{i1} \oplus \dots \oplus y_{js} = 0$ som är vanlig eller ovanlig. Fallet $0 = 0$ anses trivialt och ointressant. Vi vill med detta knäcka bitar i nyckeln.

Låt p beteckna sannolikheten att linjärapproximationen är uppfylld. Det
alt. ϵ ges av $\epsilon = p - \frac{1}{2}$. Vi vill att $|\epsilon|$ är stort. Notera att $-\frac{1}{2} \leq \epsilon \leq \frac{1}{2}$. Desto närmre bias är 0
desto större är sannolikheten att linjärapproximationen är normalfördelat.

Till en början studerar vi två bitar, x_1 och x_2 . Sannolikheten $Pr(x_i = x) = \begin{cases} p & x = 0 \\ 1-p & x = 1 \end{cases}$

Från

$$\begin{aligned} x_1 \oplus x_2 = 0 &\iff x_1 = x_2 \\ x_1 \oplus x_2 = 1 &\iff x_1 \neq x_2 \end{aligned}$$

följer att

$$Pr(x_1 = a \wedge x_2 = b) = \begin{cases} p_1 p_2 & a = 0, b = 0 \\ (1 - p_1)p_2 & a = 1, b = 0 \\ p_1(1 - p_2) & a = 0, b = 1 \\ (1 - p_1)(1 - p_2) & a = 1, b = 1 \end{cases}$$

Det ger att

$$\begin{aligned} p_{1,2} &= \\ &= Pr(x_1 \oplus x_2 = 0) \\ &= Pr(x_1 = x_2) \\ &= Pr(x_1 = 0 \wedge x_2 = 0) + Pr(x_1 = 1 \wedge x_2 = 1) \\ &= p_1 p_2 = (1 - p_1)(1 - p_2) \end{aligned}$$

Sätt $\epsilon_i = p_i - \frac{1}{2}$:

$$\begin{aligned} p_{1,2} &= \\ &= (\epsilon_1 + \frac{1}{2})(\epsilon_2 + \frac{1}{2}) + (1 - (\epsilon_1 + \frac{1}{2}))(1 - (\epsilon_2 + \frac{1}{2})) \\ &= \frac{1}{2} + 2\epsilon_1\epsilon_2 \\ &= \epsilon_{1,2} + \frac{1}{2} \\ &\Rightarrow \epsilon_{1,2} = 2\epsilon_1\epsilon_2 \end{aligned}$$

Om $x_i = 0$ är oberoende för alla $i = 1, 2, \dots, n$ så är

$$p_{1,2,\dots,n} = Pr(x_1 \oplus x_2 \oplus \dots \oplus x_n = 0) = \frac{1}{2} + 2\epsilon_1\epsilon_2 * \dots * \epsilon_n \text{ och } \epsilon_{1,2,\dots,n} = 2\epsilon_1\epsilon_2 * \dots * \epsilon_n.$$

A = alfabet. Låt n och k vara positiva heltal. Alice vill sända $x \in A^k$ (x kallas för ett) till Bob.

Hon använder en
använder

$E : A^k \rightarrow A^n$ och skickar $y = E(x)$, som kallas . Bob
 $D : A^n \rightarrow A^k$, där $D(E(x)) = x \forall x \in A^k$.

Låt $x, y \in A^n$ och $d(x, y)$ som ges av antal positioner där x och y skiljer sig åt. Exempelvis blir $d(001, 101) = 1$. Detta kallas för Hammingavstånd eller Hammingmetrik.

Notera att $d(x, y) \geq 0$ kan skrivas som $d(x, y) = 0 \iff x = y$.

Vidare är $d(x, y) = d(y, x)$ och $d(x, y) \leq d(x, z) + d(y, z)$ (triangelolikheten).

Klotet med medelpunkt i x och radien r ges av $B_r(x) = \{y \in A^n : d(x, y) \leq r\}$.

Låt $C \subseteq A^n$ vara en kod. Man säger att C kan upptäcka upp till s fel om det för varje $c \in C$ gäller att B_s endast innehåller ett kodord.

En kod C säges kunna korrigera upp till t fel om det för varje $x \in A^n$ gäller att $B_t(x)$ innehåller högst ett kodord.

Minimalavståndet definieras som $d(C) = \min(\{d(x, y) : x, y \in C \wedge x \neq y\})$. Om minimalavståndet $d(C) \geq s + 1$ så kan C upptäcka s fel. Om $d(c) \geq 2t + 1$ så kan C rätta t fel.

$$B_1(10011) = \{10011, 00011, 11011, 10111, 10001, 10010\}.$$

Låt $q = p^f$ där p är ett primtal och f ett positivt heltal. Låt \mathbb{F}_q vara den ändliga kroppen med q element.

$$\mathbb{F}_q^n = \{(v_1, v_2, \dots, v_n) : v_i \in \mathbb{F}_q\}$$

Låt $\bar{v}_1, \bar{v}_2, \dots, \bar{v}_k$ vara linjärt oberoende, d.v.s. $\lambda_1 \bar{v}_1 + \lambda_2 \bar{v}_2 + \dots + \lambda_k \bar{v}_k = \bar{0}$ har endast lösningen $\lambda_1 = \lambda_2 = \dots = \lambda_k = 0$ då $k < n$.

Bilda

$$C = \{a_1 \bar{v}_1 + a_2 \bar{v}_2 + \dots + a_k \bar{v}_k : a_i \in \mathbb{F}_q\}$$

Om $a \in \mathbb{F}_q$ och $\bar{x}, \bar{y} \in C$ så är $a\bar{x} \in C$ och $\bar{x} + \bar{y} \in C$.

Man kallar C för en linjär kod av dimension k och längden n .

Vi skriver $\bar{v} = (a_1, a_2, \dots, a_k)$.

$\text{wt}(\bar{v})$ av en vektor definieras som antalet $a_i \neq 0$.

Notera att Hammingavståndet $d(\bar{x}, \bar{y}) = \text{wt}(\bar{x} - \bar{y})$.

Sats: $d(C) = \min(\{\text{wt}(\bar{v}) : \bar{v} \in C \wedge \bar{v} \neq \bar{0}\})$.

Nu framöver använder vi oss av $\mathbb{F}_2 = \{0, 1\} \pmod{2}$. Låt P vara en $k \times (n - k)$ -matrix. Bilda $G = (I_k \ P)$ ($k \times n$ -matris). Raderna i G är linjärt oberoende. Alla kodord c fås genom att för alla $x \in \mathbb{F}_2^k$ beräkna $\bar{c} = \bar{x}G$. G kallas för en

Låt A vara en $(n - k) \times n$ -matris och $v \in \mathbb{F}_2^n$. Då gäller att $\bar{v}A^T = \bar{0} \iff v \in C$. Då kallas även A för en kontrollmatris för koden C .

Låt $H = (-P^T \ I_{n-k})$ är en kontrollmatris till C för linjära koder.

$$n = 5, k = 2, I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, P = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Ord finns i \mathbb{F}_2^2 och kodord i $\mathbb{F}_2^5 Ko$.

Kodningsavbildningen $xG, x \in \mathbb{F}_2^2$ ges av

$$\begin{aligned} (0 \ 0) \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} &= (0 \ 0 \ 0 \ 0 \ 0) \\ (0 \ 1) \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} &= (0 \ 1 \ 0 \ 1 \ 1) \\ (1 \ 0) \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} &= (1 \ 0 \ 1 \ 0 \ 1) \\ (1 \ 1) \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} &= (1 \ 1 \ 1 \ 1 \ 0) \end{aligned}$$

Hammingvikterna wt ges av

$$\text{wt}(00000) = 0$$

$$\text{wt}(01011) = 3$$

$$\text{wt}(10101) = 3$$

$$\text{wt}(11110) = 4$$

$$d(C) = \min(\{3, 3, 4\}) = 3$$

Vi noterar att $3 \geq 2 + 1$ och kan då säga att upp till två fel kan upptäckas. Vidare är $3 \leq 2 * 1 + 1$ och vi kan alltså korrigera upp till ett fel.

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\bar{v} = (11010) \notin C$$

$$\bar{v}H^T = (11010) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (100) \neq (000) \text{ (dvs. ej kodord)}$$

Se tabell.

Exempelvis $\bar{v}_3 + \bar{c}_3 = 00010 + 10101 = 10110 \pmod{2}$.

Betrakta \bar{v}_i som en störning av \bar{c}_i . Sätt $x = \bar{v}_i + \bar{c}_j$. Då är $xH^T = (\bar{v}_i + \bar{c}_j)H^T = \bar{v}_i H^T + \underbrace{\bar{c}_j H^T}_{=0} = \bar{v}_i H^T$. Det vill säga att den enda intressanta kolumnen är den första. Vi sätter $s(x) = xH^T$ som kallas syndromet för x .

Indata: $x \in \mathbb{F}_2^n$.

1. $y \leftarrow s(x)$
2. Hitta i (rad) i y förekommer
3. Returnera $c \leftarrow x + \bar{v}_i$

Från 1978. Assymetriskt krypto.

Låt G vara en (n, k) -kod likt beskrivet ovan. Låt P vara en permutationsmatris (alltså inte det P som finns i H) av ordning n (d.v.s. exakt en etta i varje rad och kolonn). Vidare låt S vara en inverterbar matris av ordning k . Sätt $G' = SGP$.

Den publika nyckeln är G' tillsammans med information om hur många fel t den kan korrigera. Privat nyckeln består av G , S och P .

Klartexten $m \in \mathbb{F}_2^k$. Efemär nyckel ges av $e \in \mathbb{F}_2^n$ med som flest t stycken ettor.

Kryptogrammet ges av $c = mG' + e$.

1. $u \leftarrow cP^{-1}$

2. Finn det $\bar{v} \in C$ som är närmast u
3. Bestäm \bar{w} så att $\bar{v} = \bar{w}G$
4. Returnera $\bar{w}S^{-1}$

$$u = cP_{\mathbb{A}}^{-1} = (mG' + e)P^{-1} = mSGPP^{-1} + eP^{-1} = mSG + eP^{-1}$$

$$v = wG = (mS)G$$

Låt $q = 2^e$ där $e \in \mathbb{N}$ och låt $\mathbb{F}_q = GF(q)$. GF är gallardkroppen.

Låt $\mathbb{F}_q \subseteq K$ och antag att K är en kropp sådan att restriktionen av addition och multiplikation i K till \mathbb{F}_q motsvarar addition och multiplikation i \mathbb{F}_q .

Man kan skriva $(K, +, *)$ för att visa att addition och multiplikation är definierat. Vi har alltså även $(\mathbb{F}_q, +, *)$ för samma operatorer.

\mathbb{F}_q kallas här för underkropp och K för kroppsutvidgning, ett vektorrum över \mathbb{F}_q .

Låt $x, y \in K$ och $a \in \mathbb{F}_q$. Då kan vi definiera vektoradditionen $x + y$ och skalärmultiplikationen ax .

Antag att K är ändligdimensionellt över \mathbb{F}_q .

Det existerar $\beta_1, \beta_2, \dots, \beta_n \in K$ sådana att alla $x \in K$ kan skrivas entydigt på formen $x = x_1\beta_1 + \dots + x_n\beta_n$ där $x_1, x_2, \dots, x_n \in \mathbb{F}_q$.

För vidare information, se kompendium från Robert Nyqvist.

Den snabbaste metoden för att faktorisera heltalet. Pollard 1988.

Givet ett sammansatt, udda heltalet n . Vi söker x och y så att $x^2 \equiv y^2 \pmod{n}$ och att $x \not\equiv y \pmod{n}$. Då är $\gcd(x - y, n)$ en möjlig icke-trivial delare till n .

Låt d vara ett positivt heltalet så att $d > 1$ och att $n > 2^{d^2}$. Sätt $m = \lfloor n^{1/d} \rfloor$. Skriv n i basen m , d.v.s. $n = c_d m + c_{d-1}m^{d-1} + \dots + c_2m^2 + c_1m + c_0$ där $c_i \in \{0, 1, \dots, m-1\}$. Vi har att $c_d = 1$.

Sätt $f(t) = c_d t^d + c_{d-1}t^{d-1} + \dots + c_2t^2 + c_1t + c_0$.

Notera att $f(m) = n$, d.v.s. $f(m) \equiv 0 \pmod{n}$. Sannolikt är $f(t)$ irreducibelt, d.v.s. det går inte att skriva $f(t) = a(t)b(t)$ där $a(t)$ och $b(t)$ är polynom med heltaletskoefficienter och båda av grad ≥ 1 .

Motivering: om det inte var fallet skulle $n = f(m) = \underbrace{a(m)}_{\in \mathbb{Z}} \underbrace{b(m)}_{\in \mathbb{Z}}$ ge ett heltalet, vilket innebär att vi faktoriserat n . Vidare faktorisering är därför onödig.

Sätt $\gamma = (\frac{8}{n})^{1/3} + \epsilon$, $\epsilon > 0$ och $B = \exp(\gamma(\log n)^{1/3}(\log \log n)^{2/3})$. Vi ska alltså studera de primtal som är mindre än B . Vidare är $d = \lfloor (\frac{2}{\gamma})^{1/2} (\frac{\log n}{\log \log n})^{1/3} \rfloor$.

Låt $\alpha \in \mathbb{C}$ vara ett nollställe till $f(t)$, d.v.s. $f(\alpha) = 0$. Låt $\alpha_1, \alpha_2, \dots, \alpha_d$ vara samtliga nollställen till $f(t)$.

Då är $f(t) = (t - \alpha_1)(t - \alpha_2)\dots(t - \alpha_d)$.

Bilda $\mathbb{Z}_{[d]} = \{x_0 + x_1\alpha^{d-1} + x_2\alpha^2 + \dots + x_{d-1}\alpha^{d-1} : x_k \in \mathbb{Z}\}$.

Notera att $\alpha^d - 1 + c_d\alpha^{d-1} + \dots + c_2\alpha^2 + c_1\alpha + c_0 = 0$ och att
 $\alpha^d = -c_{d-1}\alpha^{d-1} - \dots - c_2\alpha^2 - c_1\alpha - c_0$.

Notera också att $\mathbb{Z} \subset \mathbb{Z}_{[d]}$. Alltså fungerar aritmetiken "som vanligt" om vi enbart använder heltalen.

Om $g(t) \in \mathbb{Z}_{[d]}$ så gäller att $g(\alpha) \in \mathbb{Z}_{[\alpha]}$. Så varje $\beta \in \mathbb{Z}_{[\alpha]}$ har minst ett polynom $g(t) \in \mathbb{Z}_{[t]}$ så att $g(\alpha) = \beta$.

Låt $\sigma : \mathbb{Z}_{[\alpha]} \rightarrow \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\mathbb{Z}_n}$ enligt följande: $\sigma(\beta) = \sigma(g(\alpha)) = g(m) \pmod{n}$, d.v.s. avbilda $\beta = g(\alpha)$

på m .

- $\sigma(\beta_1 + \beta_2) = \sigma(\beta_1) + \sigma(\beta_2) \pmod{n}$
- $\sigma(\beta_1 * \beta_2) = \sigma(\beta_1) * \sigma(\beta_2) \pmod{n}$

Vi har att $\sigma(g(\alpha)^2) = \sigma(g(\alpha))^2$.

Antag att vi funnit en mängd S av polynom $g(t) \in \mathbb{Z}[t]$ sådana att $\prod_{g(t) \in S} g(\alpha) = \beta^2$ och att
 $\prod_{g(t) \in S} g(m) = y^2$.

$$S = \{g_1(t), g_2(t), g_3(t)\}. \prod_{g \in S} g(m) = g_1(m)g_2(m)g_3(m).$$

Vidare är $\sigma(\beta) \equiv x \pmod{n}$ för något heltalet x . Då är i sin tur

$$x^2 \equiv \sigma(\beta^2) = \sigma(\beta^2) = \sigma\left(\prod_{g \in S} g(\alpha)\right) = \prod_{g \in S} \sigma(g(\alpha)) = \prod_{g \in S} g(m) = y^2 \pmod{n}.$$

En talkropp definieras på följande sätt: $\mathbb{Q}(\alpha) = \{x_0 + x_1\alpha + x_2\alpha^2 + \dots + x_{d-1}\alpha^{d-1} : x_k \in \mathbb{Q}\}$.

Låt $\beta \in \mathbb{Q}(\alpha)$. Då finns det ett polynom $g(t) \in \mathbb{Q}[t]$ så att $g(\alpha) = \beta$.

Bilda $N : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}$ enligt följande: $N(\beta) = N(g(\alpha)) = \prod_{i=1}^d g(\alpha_i)$ där
 $f(\alpha_1) = f(\alpha_2) = \dots = f(\alpha_d) = 0$.

Då kallas $N(\beta)$ för normen av β .

- $N(\beta_1\beta_2) = N(\beta_1)N(\beta_2)$
- om $g(t) \in \mathbb{Z}[t]$ så är $N(g(\alpha)) \in \mathbb{Z}$

Låt a och b vara heltal där $\gcd(a, b) = 1$ och sätt $g(t) = a - bt \in \mathbb{Z}_{[t]}$.

Man säger att $a - b\alpha$ är B -milt om $N(g(\alpha)) = N(a - b\alpha)$ är B -mild. Alla primtal som delar $N(a - b\alpha)$ är mindre än B .

Vi har att $N(a - b\alpha) = \prod_{i=1}^d (a - b\alpha_i) = b^d \prod_{i=1}^d \left(\frac{a}{b} - \alpha_i\right) = b^d f\left(\frac{a}{b}\right)$.

Vi söker en mängd $S = \{(a, b) : a, b \in \mathbb{Z}\}$ vidare gäller att $\gcd(a, b) = 1$ och att $\prod_{(a,b) \in S} (a - b\alpha)$ är en kvadrat i $\mathbb{Z}[\alpha]$ (det vill säga β^2). Då är $\prod_{(a,b) \in S} N(a - b\alpha)$ en kvadrat i \mathbb{Z} (d.v.s. y^2).

R är en ring, $I \subseteq R$. Om $ab \in I$ för alla $a \in R$ och alla $b \in I$ och $(I, +)$ är en grupp, så säges I vara ett ideal till R .

Lått \mathbb{F} vara en kropp och $I \subset F[X_1, X_2, \dots, x_m]$ ett ideal.

Låt $f_1, f_2, \dots, f_l \in [\bar{X}]$ och låt I vara de element som skrivs som en linjärkombination av f_1, f_2, \dots, f_l .

Denna mängd I är ett ideal och man skriver $I = (f_1, f_2, \dots, f_l)$ och säger att I genereras av $F = \{f_1, f_2, \dots, f_m\}$.

Låt \mathbb{F} vara en algebraiskt sluten kropp och I ett icke-trivialt ideal till $\mathbb{F}[\bar{X}]$ med ett givet antal variabler. Då existerar det ett element $\bar{a} = (a_1, a_2, \dots, a_m) \in \mathbb{F}^m$ så att $f(\bar{a}) = 0$ för alla $f \in I$.

Grad-lexikongrafisk ordning i först m.a.p. totalgrad och sedan i bokstavsordning.

Mn sägera att f reduceras till $h \mod g$ i ett steg om $a_i \bar{X}^i$ är delbar med $lt(g)$ och $h = f - \frac{a_i \bar{X}^i}{lt(g)} g$. Med $lt(g)$ menas den ledande termen efter reducering.

Man skriver $f \rightarrow^g h$. Viktigt specialfall: $h = f - \frac{lt(f)}{lt(g)} g$ tack $lt(h) < lt(f)$.

$$\begin{aligned} f(X, Y, Z) &= X^4 + XY^2Z = XXXX + XYZ = X^4 + XY^2Z \\ f(X, Y, Z) &= X^2Y - X^2Z + XYZ = XXY - XXZ + XYZ = X^2 - X^2 + XYZ \\ g_1 &= X^3 - XZ, lt(g) = X^3 \\ h_1 &= f - \frac{x^4}{x^3}g = X - XY + X^2Y + Y^2 - xY^2 - Z + YZ + XYZ - Z^2 \\ g_2 &= XY^2 + YZ, lt(g_2) = XY^2 \dots \end{aligned}$$

Låt $F = \{g_1, g_2, \dots, g_l\} \subseteq \mathbb{F}[\bar{X}]$ och $I = (g_1, g_2, \dots, g_l)$. Då säges F vara en gröbnerbas för I om det för varje $f \in I$ gäller att $\text{lt}(g_i) | \text{lt}(f)$ för alla $i = 1, 2, \dots, l$.

S -polynomet för f och g ges av $S(f, g) = \frac{L}{\text{lt}(f)} f - \frac{L}{\text{lt}(g)} g$ där $L = \text{lcm}(\text{lt}(f), \text{lt}(g))$.

$$\begin{aligned} f &= X^2Y - XZ + Y \\ g &= XY^2 + YZ \\ L &= X^2Y^2 \\ S(f, g) &= \frac{X^2Y^2}{X^2Y} f - \frac{X^2Y^2}{XY^2} g = Y^2 - 2XYZ \end{aligned}$$

F är en gröbnerbas om och endast om $S(g_i, g_j)$ reduceras till 0 för varje $i \neq j$ i ett eller flera steg.

Reducera vare $S(g_i, g_j)$ till $h_{i,j}$ med hjälp av polynomen i F . Om $h_{i,j} \neq 0$ så läggs $h_{i,j}$ till F . Efterhand läggs polynomen g_{l+1}, g_{l+2}, \dots , till. Upprepa tills dess att alla $S(g_i, g_j), i \neq j$ reduceras till 0.

Denna algoritm avbryter efter ett ändligt antal steg och F är en gröbnerbas.

En gröbnerbas $\{g_1, g_2, \dots, g_l\}$ säges vara minimal om varje g_i är monisk, det vill säga den inledande termen har en etta som koefficient. Dessutom måste $\text{lt}(g_i) \nmid \text{lt}(g_j)$ då $i \neq j$.

Om t.ex. $\text{lt}(g_1) | \text{lt}(g_l)$ så kan vi ersätta g_l med h då $g_l \rightarrow^{g_1} h$. h är en linjärkombination av g_1, g_2, \dots, g_{l-1} och $\text{lt}(h) < \text{lt}(g_l)$. Dessutom vet vi att $h \in I$.

En gröbnerbas är reducerad om varje g_i är monisk och ingen term i g_i är delbar med $\text{lt}(g_j)$ då $i \neq j$.

Först reduceras g_1 med hjälp av g_2, \dots, g_l till något h_1 som ersätter g_1 . Reducera g_2 med hjälp av h_1, g_3, \dots, g_l till h_2 . Ersätt g_2 med h_2 . Förstått för övriga g_i .