MATEMATIKKEN BAK GPS, DET GLOBALE POSISJONERINGSSYSTEM

RAGNAR SOLENG

Abstract. Det kostet 12 milliarder dollar å lage, men så har vi omsider fått et navigeringssystem som virker uansett hvorhen på kloden du er. I denne artikkelen skal vi først se på hvordan man kompenserer for unø yaktighet i klokkene ved å bruke en fjerde satelitt. Deretter skal vi forklare hvordan avstander fra satelitter til GPS-mottaker måles og spesielt se på matematikken i dette.

1. Innledning

Mennesket er fra naturens side dyra overlegen på en rekke områder. Evnen til å finne fram i ukjent terreng er ikke blant disse. Fugler kan fly i tåke over store havstrekninger og finne nøyaktig tilbake til reiret. Selv fisker kan svømme rundt i verdenshavene i årevis for deretter å legge turen tilbake til elven som de engang var født i.

Slike naturgitte egenskaper har ikke mennesket. Derfor har vi hele tiden prøvd å finne på ting som kan helpe oss til å navigere rett. Det er brukt enorme ressurser i tid og penger for å tegne kart over hver en avkrok av jordkloden. Med et slikt kart kan en i klarvær til enhver tid holde nøaktig rede på hvor en er. Tar man også med et kompass på turen vet en også hvilken retning en skal gå for å komme dit en skal.

Men i noen situasjoner hjelper det lite å ha kart. Legger du turen inn over vidda en vinterdag har kart liten mening. Et hvitt A4 ark fungerer like godt. Det samme gjelder om en vil krysse store havstrekninger.

Den tradisjonell metoden for navigering i slike situasjoner er å bruke sekstant og klokke. Måler du solhøyden ved vårjevndøgn midt på dagen til x grader, dvs. vinkelen sola danner med horisonten når sola er på sitt høyeste, så viser litt ungdomsskolegeometri at breddegraden du er på er $90 - x$ (Hvis det ikke er vår- eller hø stjevndøgn må man korrigere for dette). Hvis du i tillegg ser at din klokke er 2PM,- ja, så vet du at du er to timer vest i havet, som er det samme som 30 grader.

Hovedproblemet med en slik navigeringsmetode er nøyaktighet. Solhøyden skal måles på minutters nøyaktighet i urolig sjø og uansett er en avhengig av klarvær. Dessuten trenger du en nøyaktig klokke [1].

Flere avanserte metoder (LORAN, OMEGA, NavSat) har vært brukt. Felles for disse er at de har vært dyre for utbyggerne og derfor har hatt dårlig dekning, eller de har vært dyre for brukerne og derfor ikke vært noe for hvermann.

[1]Historisk har problemet med å utvikle nøyaktige klokker vært stø rst. Dette ble løst på 17-hundretallet da John Harrison utviklet sin presise klokke $H4$, og dermed kunne gjøre krav de $ 2000 som var utlovet til den som kunne finne en metode til å bestemme lengdegraden. Se Dava Sobel ,[3].

Så, som en del av våpenkappløpet under den kalde krigen bestemte US Department of Defence seg for å lage et posisjoneringssystem slik at deres ubåter kunne dukke opp hvor som helst, bestemme sin posisjon nøyaktig i løpet av minutter, for deretter å avfyre sine våpen. Våpnene i seg selv var allerede blitt så nøyaktige at de kunne treffe hva som helst bare de visste hvor de ble avfyrt fra.

Systemet kostet 12 milliarder dollar å bygge ut, og er heldigvis gjort tilgjengelig for alle[2]. Og hva som er enda hyggeligere, er at utstyret du og jeg trenger for å bruke systemet er billig. Det koster i dag fra 1500 kroner og oppover, men blir stadig billigere. Systemet heter GPS, det globale posisjoneringssystem.

2. Det globale posisjoneringssystem

Systemet består av:

24 satelitter i nøyaktig bestemte baner rundt jorden.

Disse sendeer kontinuerlig signaler til GPS mottakere verden over.

5 bakkestasjoner: Hawaii, Ascension Island, Diego Garcia, Kwajalein og Colorado Spring

Disse følger satellittene nøye og korrigerer for unøyaktigheter i bane og klokke.

3. Virkemåte

For at din GPS mottaker skal kunne gi deg nøyaktig posisjon må den ha signal fra minst 3 satellitter. Den måler tiden signalet tar fra satellitten til mottakeren og siden signalet går med lysets hastighet er avstanden r lett å regne ut. Avstanden til den første satellitten forteller mottakeren at den befinner seg et eller annet sted på en kuleflate med radius r fra satellitten. Tar du i betraktning avstanden til den andre sattellitten også, så vet du at du befinner deg i skjæ ringen mellom to sfærer, som er en sirkel. Den tredje sattellitten innskrenker mulighetene til to punkter på denne sirkelen. En fjerde sattellitt ville bestemme hvilket av disse posisjonene som er rett, men det er unødvendig siden det ene av punktene vil ligge langt ute i verdensrommet.

Prinsippet for GPS er altså enkelt. I virkeligheten er det mange vanskeligheter som må overkommes. Noen av disse har matematiske lø sninger.

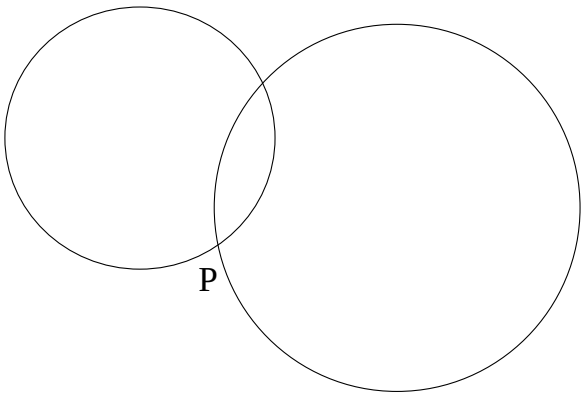
4. Unøyaktigheter i klokkene

Satellittene er utstyrt med nøyaktige atomur som angir universell tid med stor nøyaktighet. I tillegg korrigeres de jevnlig fra bakkestasjonene slik at unøyaktighet i satellittklokkene ikke utgjør mer enn ca. 10^{-8} sekund per døgn, som igjen gir en meters unøyaktighet i posisjonsbestemmelsene.

Dessverre har ikke GPS-mottakeren klokke av samme kvalitet, det ville bli for dyrt. Heldigvis er det heller ikke nødvendig. Måling fra en fjerde satellitt fjerner feil som skyldes unøyaktighet i mottakerklokken nesten helt. Vi skal senere se hvordan dette kan gjøres algebraisk, men først skal vi vise med noen tegninger hvordan en

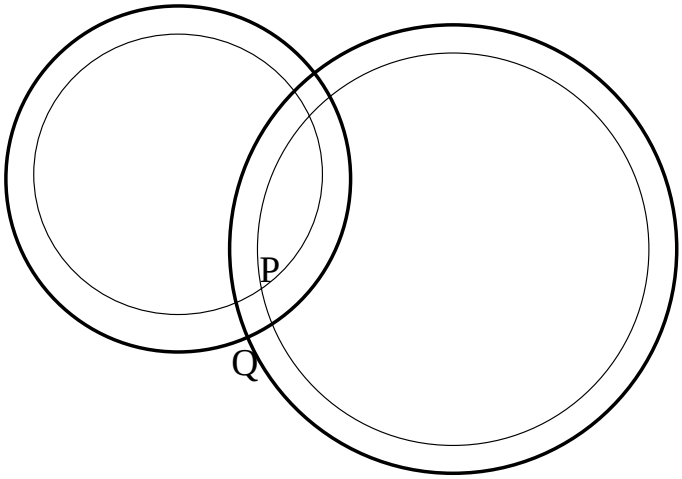
[2]Dette er ikke helt rett. Systemet sender på to frekvenser. Signalet i den som er tilgjengelig for alle er lagt til en vilkårlig feil slik at nø yaktigheten ikke er større en 100 meter.

fjerde måling fjerner unø yaktigheten. For enkelhets skyld skal vi gjøre dette i to dimensjoner hvor 2 satellitter er nok til å bestemme posisjon, men en tredje måling fjerner feil fra unøyaktighet i mottakerklokka helt.



Figur 1

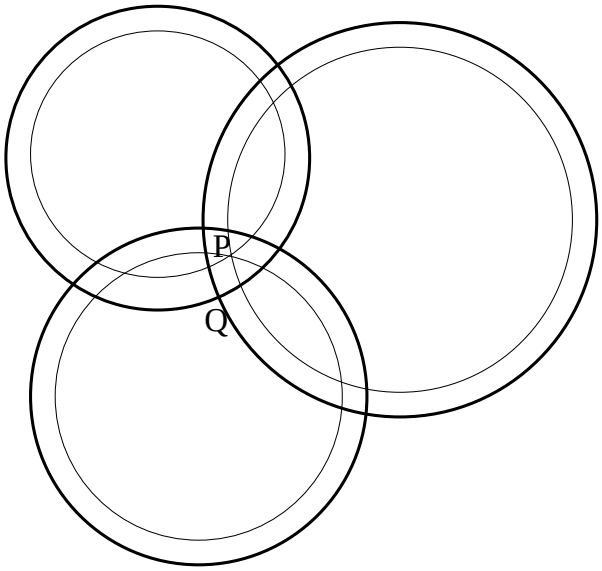
La oss anta at vår posisjon er 3 sekunder fra satellitt A og 5 sekunder fra satellitt B. Så anta at punktet P i figur 1 er vår posisjon. Denne posisjonen ville vår GPS-mottaker finne om den hadde en nøyaktig klokke. Men anta at klokka går ett sekund for sakte, dermed ville avstanden til A måles til 4 sekunder mens avstanden til B blir 6 sekunder. Disse to sirklene ville skjære i et feilt punkt Q, se figur 2.



Figur 2

Så hva hjelper det nå å foreta en tredje måling (eller fjerde i det tredimensjonale tilfelle)?

Hvis klokka i mottakeren hadde vært rett ville alle målingene gå gjennom punktet P som er vår riktige posisjon. Med en klokke som er ett sekund for sein ser bildet ut som på figur 3.



Figur 3

Legg merke til at ytre sirklene ikke skjærer hverandre i noe felles punkt. Dette faktum forteller oss at det er noe feil i målingene. Det GPS-mottakeren gjør nå er å lete etter en passende korreksjon til klokka som ville få alle sirklene til å skjære i ett felles punkt. I dette tilfelle, ett sekund.. Dett er mulig siden tidsfeilen i alle tre målingne kan antas å være den samme. Vi skal nå se hvordan dette gjøres algbraisk. Det finnes flere forskjellige fremgangsmåter, vi skal velge en metode foreslått av Bancroft i 1985.

5. Beregning av posisjon

Vi følger framstillingen i [1].

La $\mathsf{r} = (x, y, z)$ og $\mathsf{r}_k = (x_k, y_k, z_k)$ være koordinatene til henholdsvis mottakeren og satellitt. Vi skriver r_k for å indikere at det er flere satellitter, minst $k = 1, 2, 3, 4$. Satellittenes koordinater er kjent mens vi ønsker å beregne r. Avstanden mellom satellitten og mottakeren er gitt ved

$$\sqrt{(x - x_k)^2 + (y - y_k)^2 + (z - z_k)^2},$$

men fordi klokka i mottakern ikke er rett måler vi egentlig avstanden

$$d_k = \sqrt{(x - x_k)^2 + (y - y_k)^2 + (z - z_k)^2} + cdt.$$

Her er c lyshastigheten og dt er feilen klokka i GPS-mottakeren står for. For å spare tastetrykk skal vi i fortsettelsen skrive $b = cdt$.

Flytter vi $b = cdt$ over på venstre side og kvadrerer får vi

$$d_k^2 - 2d_k b + b^2 = x^2 - 2xx_k + x_k^2 + y^2 - 2yy_k + y_k^2 + z^2 - 2zz_k + z_k^2.$$

Nå samler vi de kjente størrelsen for seg

$$(x_k^2 + y_k^2 + z_k^2 - d_k^2) - 2(x_k x + y_k y + z_k z - d_k b) + (x^2 + y^2 + z^2 - b^2) = 0.$$

For de som kan noe om matriser og skalarprodukt fra lineæralgebraen finnes det en alternativ måte å skrive dette på. La

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

og definer et skalarprodukt $\langle \mathsf{a}, \mathsf{b} \rangle = \mathsf{a}^t M \mathsf{b}$ for vektorer a og b i R^4. Da kan ligningen over skrives som

$$\frac{1}{2}\left\langle \begin{pmatrix} \mathsf{r}_k \\ d_k \end{pmatrix}, \begin{pmatrix} \mathsf{r}_k \\ d_k \end{pmatrix} \right\rangle - \left\langle \begin{pmatrix} \mathsf{r}_k \\ d_k \end{pmatrix}, \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix} \right\rangle + \frac{1}{2}\left\langle \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix}, \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix} \right\rangle = 0.$$

Vi innfører ytterligere notasjon og setter $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ hvor

$$\alpha_k = \frac{1}{2}\left\langle \begin{pmatrix} \mathsf{r}_k \\ d_k \end{pmatrix}, \begin{pmatrix} \mathsf{r}_k \\ d_k \end{pmatrix} \right\rangle, \quad k = 1, 2, 3, 4.$$

Dessuten definerer vi

$$B = \begin{pmatrix} x_1 & y_1 & z_1 & d_1 \\ x_2 & y_2 & z_2 & d_2 \\ x_3 & y_3 & z_3 & d_3 \\ x_4 & y_4 & z_4 & d_4 \end{pmatrix}, \Lambda = \frac{1}{2}\left\langle \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix}, \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix} \right\rangle$$

og $\mathsf{e} = (1, 1, 1, 1)$. Da kan ligningssettet skrives

$$\boldsymbol{\alpha} - BM \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix} + \Lambda \mathsf{e} = \mathsf{0}.$$

Her er $\begin{pmatrix} \mathsf{r} \\ b \end{pmatrix}$ de ukjente og løsningen kan skrives

$$(*) \qquad \begin{pmatrix} \mathsf{r} \\ b \end{pmatrix} = MB^{-1}(\Lambda \mathsf{e} + \boldsymbol{\alpha}).$$

Dette ser ikke helt bra ut siden de ukjente størrelsene $\begin{pmatrix} \mathsf{r} \\ b \end{pmatrix}$ også inngår i Λ. Men se hva som skjer hvis vi setter uttrykket (*) inn i uttrykket for Λ og husker at $\langle M\mathsf{a}, M\mathsf{b} \rangle = \langle \mathsf{a}, \mathsf{b} \rangle$. Da får vi følgende annengradsligning for Λ :

$$\left\langle B^{-1}\mathsf{e}, B^{-1}\mathsf{e} \right\rangle \Lambda^2 + 2\left\langle B^{-1}\mathsf{e}, B^{-1}\boldsymbol{\alpha} \right\rangle + \left\langle B^{-1}\boldsymbol{\alpha}, B^{-1}\boldsymbol{\alpha} \right\rangle = 0.$$

Denne har to løsninger, hvorav den ene gir oss korrekt posisjon mens den andre angir en posisjon lang ute i verdensrommet.

Hvis GPS-mottakeren opererer med signaler fra flere enn fire satellitter, noe de fleste gjør, må algoritmen justeres noe.

6. Måling av avstand

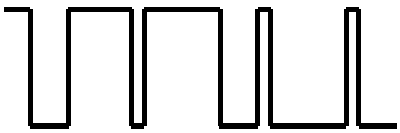
For å måle avstanden fra satellitten til mottakeren utnytter man det faktum at alle signaler, enten det er lyd, lys eller radiosignaler, beveger seg med en endelig og noenlunde konstant fart. Hvis man kan måle tiden signalet har brukt fra satelitt til mottaker, finner man lett avstanden ved å multiplisere farten med tiden. Så det er nok å kunne måle tiden et radiosignal trenger fra satellitten til GPS-mottakeren. Hvordan gjøres så det? Det er overraskende, men man bruker en tilfeldig tall generator for dette. I dette tilfellet, en generator som produserer sekvenser av 0-ere

og 1-ere på en slik måte at det ser ut som de er trukket helt tilfeldig. Tradisjonelt har slike vært brukt til å teste statistiske modeller og også til kryptering av meldinger

Satellitten sender altså et signal som er styrt av en tilfeldig tall generator. Et eksempel er sekvensen

$$1101111101101010010011 0 \ldots .$$

Signalet startes på et kjent tidspunkt og hver klokkepuls sendes en 0 eller en 1 alt etter hva som er neste tall i sekvensen. I virkeligheten sendes et analogt signal som ser ut som på figur 4.



Figur 4

I GPS-mottakeren finnes samme tilfeldig tall generator. Mottakeren sammenligner sin sekvens med signalet som kommer fra satellitten og oppdager at det er en tidsforsinkelse i dette. Denne forsinkelsen kan ikke skyldes annet enn at signalet har reist langt. Det har reist med lysets hastighet c og hvis tidsforsinkelsen måles til t, så er avstanden mellom satellitten og mottakeren lik $d = ct$.

Legg merke til at dette er nøyaktig samme prinsipp som når vi teller antall sekunder mellom lynglimt og tordenbrak for å anslå avstanden til lynnedslaget. Da multipliserer vi antall sekunder med lydens hastighet.

I neste de neste avsnittene skal vi se litt nærmere på den typen tilfeldig tall generator som brukes i GPS-systemet.

7. Lineære skift registre

Den tilfeldig tall generatoren som brukes i GPS-systemet er en såkalt Linear Feedback Shift Register (LFSR) av blokklengde 10. Faktisk brukes det to slike, og militæret i USA har sitt eget signal som bruker en LFSR av lengde 12.

La oss nå se på hvordan en LFSR virker. Som startverdi har vi et register av lengde 10 med 0-ere og 1-ere, for eksempel

$$[1]\,[0]\,[0]\,[0]\,[1]\,[1]\,[0]\,[1]\,[1]\,[1]$$

Ved hver klokkepuls leses tall nr. 1 ut og alle tallene flyttes en posisjon til venstre. Da får vi en ledig plass i siste posisjon i registret.

$$[0]\,[0]\,[0]\,[1]\,[1]\,[0]\,[1]\,[1]\,[1]\,[\ ]\,.$$

Denne skal gis verdi tilsvarende en lineær sum av de 10 foregående tallene. For eksempel sum av tall nummer 3 og 10. Vi regner modulo 2 slik at $0 + 0 = 0$, $1 + 0 = 1$ og $1 + 1 = 0$. Etter én, to, tre og fire klokkepulser blir registret seende slik ut

$$\begin{gathered}[0]\,[0]\,[0]\,[1]\,[1]\,[0]\,[1]\,[1]\,[1]\,[1]\\ [0]\,[0]\,[1]\,[1]\,[0]\,[1]\,[1]\,[1]\,[1]\,[1]\\ [0]\,[1]\,[1]\,[0]\,[1]\,[1]\,[1]\,[1]\,[1]\,[0]\\ [1]\,[1]\,[0]\,[1]\,[1]\,[1]\,[1]\,[1]\,[0]\,[1]\,,\end{gathered}$$

og tallene som leses ut er 10001.

Dette er faktisk den ene av de to LFRSR som brukes. Det kan vises at etter 1023 klokkepulser står vi igjen med det registret vi startet med, vi sier at denne LFSR har periode 1023. Vi skal senere se på hvordan perioden kan regnes ut.

De verdiene som leses ut av registret utgjør en følge av binære tall $\{a_0, a_1, a_2, \ldots\}$. Den lineære feedback kan skrives som en rekursjonsligning

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r}$$

hvor hver av koeffisientene $c_1, c_2, c_3, \ldots, c_r$ er 0 eller 1 og ikke avhenger av n. Startverdiene betegner vi med $a_{-r}, a_{-r+1}, \ldots, a_{-1}$. I eksemplet over er $r = 10$.

Eksempel 1. Som et eksempel ser vi på et LFSR av lengde 4 hvor startverdiene er 1,0,0,0 og rekursjonsligningen er

$$a_n = a_{n-1} + a_{n-4}.$$

Følgen av tall som leses ut blir da $\{1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0\}$. Vi ser at etter 15 klokkepulser er vi tilbake til startpunltet. Etter dette vil sekvensen gjenta seg. Vi sier at registret har periode 15. Legg merke til at perioden kan skrives som $2^4 - 1$ noe vi straks skal se er typisk.

7.1. Genererende funksjon. Den genererende funksjon for et skiftregister $\{a_0, a_1, a_2, \ldots\}$ er

$$G(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Siden $\{a_0, a_1, a_2, \ldots\}$ tilfredsstiller rekursjonsligningen

$$a_n = \sum_{i=1}^{r} c_i a_{n-i}$$

får vi

$$\begin{aligned} G(x) &= \sum_{n=o}^{\infty} \sum_{i=1}^{r} c_i a_{n-i} x^n \\ &= \sum_{i=1}^{r} c_i x^i \sum_{n=0}^{\infty} a_{n-i} x^{n-i} \\ &= \sum_{i=1}^{r} c_i x^i (a_{-i} x^{-i} + \cdots a_{-1} x^{-1} + G(x)). \end{aligned}$$

Litt enkel algebra gir nå at

$$G(x) = \frac{\sum_{i=1}^{r} c_i x^i (a_{-i} x^{-i} + \cdots a_{-1} x^{-1})}{1 - \sum_{i=1}^{r} c_i x^i}.$$

Polynomet $f(x) = 1 - \sum_{i=1}^{r} c_i x^i$ kalles det karakteristiske polynomet til registret.

Eksempel 2. De to LFSR som brukes i GPS-systemet (sivil del) har karakteristiske polynom $1 + x^3 + x^{10}$ (som blir referert til som G1) og $1 + x^2 + x^3 + x^6 + x^8 + x^9 + x^{10}$ (G2). Hver enkelt satellitt bruker en "vridd" versjon (output tas på en spesiell måte) av G2 som legges sammen binært med G1. Resultatet er satellittens karakteristiske signal som sendes kontinuerlig. Signalet er periodisk med en periode på ca. 1,5 sekunder. "Vridningen" av G2 gjøres forskjellig for hver satellitt slik at hver satellitts signal er lett gjenkjennelig.

Militæret har sitt eget signal som er periodisk med en ukes lengde.

7.2. **Perioden til en LFSR.** For en LFSR av lengde r er det 2^r mulige tilstander for registret. Det er fordi det på hver plass i registeret kan stå enten en 0 eller en 1. Tilfellet hvor alle plassene er 0 resulterer opplagt i bare nullere i framtiden også, så denne har periode 1. For andre LFSR er da det maksimale antall tilstander lik $2^r - 1$ og dette er dermed den maksimale perioden til et register. For hver r finnes registre med maksimal periode.

Teorem 1. Anta $\{a_0, a_1, a_2, \ldots\}$ har startverdier $a_{-1} = a_{-2} = \cdots = a_{-r+1} = 0, a_{-r} = 1$. Da er perioden til $\{a_0, a_1, a_2, \ldots\}$ lik det minste heltall p slik at $f(x)$ deler $1 - x^p$.

Bevis. Fordi startverdiene er som de er har vi at $G(x) = \sum a_n x^n = \frac{1}{f(x)}$. Hvis perioden er lik p så er

$$\begin{aligned}\frac{1}{f(x)} &= a_0 + a_1x + a_2x^2 + \cdots a_{p-1}x^{p-1} + x^p(a_0 + a_1x + a_2x^2 + \cdots a_{p-1}x^{p-1}) \\ &\quad + x^{2p}(a_0 + a_1x + a_2x^2 + \cdots a_{p-1}x^{p-1}) + \cdots \\ &= (a_0 + a_1x + a_2x^2 + \cdots a_{p-1}x^{p-1})(1 + x^p + x^{2p} + x^{3p} + \cdots \\ &= (a_0 + a_1x + a_2x^2 + \cdots a_{p-1}x^{p-1})\frac{1}{1 - x^p}.\end{aligned}$$

Så $f(x)(a_0 + a_1x + a_2x^2 + \cdots a_{p-1}x^{p-1}) = 1 - x^p$. Dvs., $f(x)$ deler $1 - x^p$ som var det vi skulle bevise. Motsatt anta $f(x)$ deler $1 - x^q$ og at kvotienten er $b_0 + b_1x + b_2x^2 + \cdots + b_{q-1}x^{q-1}$. Da er

$$\begin{aligned}G(x) &= \frac{1}{f(x)} = \frac{b_0 + b_1x + b_2x^2 + \cdots + b_{q-1}x^{q-1}}{1 - x^q} \\ &= (b_0 + b_1x + b_2x^2 + \cdots + b_{q-1}x^{q-1})(1 + x^q + x^{2q} + x^{3q} \ldots\end{aligned}$$

Siden $G(x) = a_0 + a_1x + a_2x^2 + \cdots$ viser dette at $q = p$ og at $a_i = b_i$ for alle i og at perioden er p. ¤

Generelt er $G(x) = \frac{g(x)}{f(x)}$ hvor $g(x)$ har lavere grad enn $f(x)$, og $f(x)$ kan antas å ha grad r. Hvis $g(x)$ ikke har felles faktorer med $f(x)$, for eksempel hvis $f(x)$ er irredusibelt (kan ikke faktoriseres i lavere grads polynomer), så gjelder teoremet over like godt. Vi ser her bort fra den uinteressante situasjonen at $g(x)$ er nullpolynomet, dvs. at man starter med bare nullere.

Vi skal nå angi en nødvendig, men ikke tilstrekkelig betingelse for at registeret skal ha maksimal periode.

Teorem 2. Hvis $\{a_0, a_1, a_2, \ldots\}$ har maksimal periode $p = 2^r - 1$, så er $f(x)$ irredusibelt.

Bevis. Siden perioden $p = 2^r - 1$ er maksimal finnes alle sekvenser av nullere og enere av lengde r untatt den med bare nullere. Spesielt finnes et sted en ener etterfulgt av $r-1$ nullere. Hvis vi starter her er teorem 1 oppfylt, så p er minste heltall q slik at $f(x)$ deler $1-x^q$. Anta nå at $f(x)$ er redusibelt, dvs $f(x) = s(x)t(x)$. Såfremt $s(x)$ og $t(x)$ ikke har felles faktorer kan vi foreta en delbrøkoppspalting og skrive

$$\frac{1}{f(x)} = \frac{1}{s(x)t(x)} = \frac{\alpha(x)}{s(x)} + \frac{\beta(x)}{t(x)}.$$

La $s(x)$ ha grad r_1 og $t(x)$ ha grad r_2 slik at $r = r_1 + r_2$ er graden til $f(x)$. Da er $\frac{\alpha(x)}{s(x)}$ en potensrekke som har periode høyst $2^{r_1} - 1$ og $\frac{\beta(x)}{t(x)}$ har høyst periode $2^{r_2} - 1$. Summen $\frac{1}{f(x)}$ er da en potensrekke med periode høyst lik minste felles multiplum av $2^{r_1} - 1$ og $2^{r_2} - 1$. Siden minste felles multiplum er mindre enn produktet har vi at

$$\begin{aligned} 2^r - 1 &\leq (2^{r_1} - 1)(2^{r_2} - 1) = 2^{r_1 + r_2} - 2^{r_1} - 2^{r_2} + 1 \\ &\leq 2^r - 2 - 2 + 1 = 2^r - 3 \end{aligned}$$

Denne ulikheten er ikke riktig, så $f(x)$ må være irredusibel. Tilfellet hvor $s(x)$ og $t(x)$ har felles faktorer overlates til leseren. ¤

Eksempel 3. Eksemplet på side 7 har maksimal periode. Det karakteristiske polynonet $1 + x + x^4$ er irredusibelt. Polynomet $1 + x + x^2 + x^3 + x^4$ er irredusibel, likevel har den tilhørende følgen periode 5.

7.3. **Mercenne primtall.** Vi skal avslutte om lineære skiftregistre med å si litt om Mercenne primtall. Et Mercenne primtall er et primtall på formen $2^n - 1$. Det er funnet mange slike og verdensrekorden er når dette skrives $q = 2^{6972593} - 1$. Det er et faktum at ethvert irredusibelt polynom (modulo 2) av grad r, må dele polynomet $1 - x^{2^r - 1}$. Teorem 1 forteller oss at perioden til et LFSR er minste heltall p slik at $f(x)$ deler $1 - x^p$. Det følger at p må gå opp $2^r - 1$. Den enkleste måten å se dette på er antagelig følgende. Røttene til $1 - x^p$ er p'te rø tter av 1. Så da må røttene til $f(x)$ være det også. Men siden røttene til $1 - x^{2^r - 1}$ er $2^r - 1$'te røtter av 1 er røttene til $f(x)$ både p'te røtter og $2^r - 1$'te røtter av 1. Så da må p gå opp $2^r - 1$. Vi har da bevist følgende teorem.

Teorem 3. Hvis det karakteristisk polynom $f(x)$ til en følge er irredusibelt av grad r, så er perioden en faktor i $2^r - 1$.

Korollar 1. Hvis $2^r - 1$ er et primtall, så korresponderer ethvert irredusibelt polynom av grad r til et skift register av maksimal lengde $2^r - 1$.

Å finne stadig nye Mersenne primtall har blitt en verdensomspennende sport. Det gleder oss å vite at de også har praktisk betydning.

8. Kjente feilkilder

I dette avsnittet lister vi de viktigste feilkildene for GPS-systemet. For sivile standard GPS-mottakere er Selective Availability (SA) den absolutt viktigste. USAs president har bestemt at denne skal fjernes innen år 2006. Vi håper det skjer.

Typiske feil målt i meter (per satellitt)

	Standard GPS	Differensiell GPS
Satelittklokke	1,5	0
Banefeil	2,5	0
Ionosfære	5,0	0,4
Troposfære	0,5	0,2
Mottakerstøy	0,3	0,3
Multipath	0,6	0,6
SA	30 (slått av 1. mai 2000)	0

Posisjonsnøyaktighet

	Standard GPS	Differensiell GPS
Horisontal	50	1,3
Vertikal	78	2
3D	93	2,8

References

[1] Gilbert Strang og Kai Borre: Linear algebra, Geodesy and GPS
[2] Solomon W. Golomb: Shift Registers Sequences
[3] Dava Sobel: LONGITUDE, The Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time. Penguin Book
[4] Trimble GPS Tutorial: www.trimble.com/gps/fsections/a_f1.htm

Universitetet i Tromsø
E-mail address: ragnar@math.uit.no
URL: http://www.math.uit.no/~ragnar