

Framhaldsskólinn í Vestmannaeyjum

Notkun brotamynda í tætisgrímum

(usage of fractals in hashing algorithms)

- Rannsóknarritgerð í STÆ513 -

Smári Páll McCarthy
Guðmundur Daði Haraldsson
STÆ513
Vorönn 2003

Nokkur aðfararorð

Flutningur gagna og áreiðanleiki hans hefur orðið mörgum að umhugsunarefni og jafnframt aldurtíla. Gögn sem komast til skila, en eru ekki í fullri lengd eða skemmd á einhvern hátt eru oftast en ekki lítils virði eða jafnvel ónothæf fyrir þann sem þarf að nota þau. Og hér er þá spurningin, hvaða aðferðir eru hentugar til að sjá til þess að þessir tveir þættir gagnaflutninga séu í lagi? Mögulegt svar er að senda gögnin aftur til baka frá upprunastað sínum og fá staðfestingu á að gögnin hafi raunverulega verið eins og móttakandinn fékk þau, en þetta er ekki hentugt þar sem þetta þarfnast þess að senda gögnin tvisvar sinnum og fyrir utan það þá gætu gögnin skemmst í flutningnum í annað skiptið! Mun hentugri leið er að nota aðferð sem býr til einkennandi munstur, stafi eða eitthvað slíkt úr gögnunum og senda það fyrir eða á eftir gagnastraumnum til að móttakandinn geti staðfest með notkun þess að gögnin séu í upprunalegri mynd.

Og þá erum við komin niður á það sem við ætlum okkur að fjalla um í þessu riti: staðfesting gagnainnihalds með sambland af notkun á brotamyndum (e. fractals) og tætisgríma (e. hashing functions). Tætisgrímar eru vel þekktir innan tölvugeirans og hafa verið notaðir mikið þar til staðfestingar á gagnaflutningi. En það að blanda saman notkun á brotamyndum og tætisgrímum er eitthvað sem er nýtt fyrir okkur báðum og okkur langar að leika okkur aðeins með. Árangurinn gæti orðið fróðlegur og lærdómsríkur.

Aðdragandinn að því að við fórum að spá í brotamyndum og tætisgrímum er nokkur, nokkrum misserum fyrr hafði Smári verið að spá talsvert í brotamyndum (og þá einkum Mandelbrot) en Guðmundur hafði talsvert spáð í tætisgrímum. Við vissum að við máttum skrifa um hvað sem er í lokaritgerðinni okkar, svo framarlega sem það snérist um stærðfræði á einhvern hátt. Vissulega á þetta tvennt sér bæði sterkar rætur í stærðfræði og fékk Smári þá hugmynd að skella þessum tveimur þáttum saman og skrifa ritgerðina um það, og það varð úr. Það sem meira er varðandi þetta er það að okkur til mikillar furðu var þessi samsetning á tveimur af flóknari greinum stærðfræðinnar nákvæmlega sú lausn sem að við höfðum verið að leita að deginum áður, þegar að verið var að ræða um hugsanlegar aðferðir við að hafa samhverfan tætisalgrím á rásinni #C.is á IRCnet, hugmynd sem að Davíð Steinn Geirsson kom með. Við komumst þá að þeirri niðurstöðu að slíkt væri ómögulegt, en höfum ekki látið okkur detta í hug notkun brotamynda.

Það myndi ekki hæfa samvisku okkar að segja annað en að rannsóknir okkar á þessu viðfangsefni eru ekki tæmandi, en fyrstu niðurstöður okkar eru athyglisverðar að okkar mati. Við tókum ef til vill of flókið umræðuefni, en það skiptir ekki neinu máli, vegna þess að í versta falli lærum við eitthvað af þessu, og í besta falli kollvörpum við einhverri kenningu. Hvað ætli gullni meðalvegurinn leiði af sér í þetta skiptið?

Kynning á brotamyndum

Almennt um brotamyndir

Þegar Benoit B. Mandelbrot starfaði sem stærðfræðingur hjá IBM árið 1958 var hann beðinn um að leysa það óþolanlega vandamál að handahófskenndar truflanir komu fram í sendingu boða. Samstarfsmenn hans höfðu skýringu á þessu; að það væru menn með skrúfjárn að vinna einhverstaðar í netkerfinu.

Mandelbrot svaraði: "Ég vil ekki heyra neinar kenningar núna. Það eru alltaf gaurar með skrúfjárn, en við munum aldrei vita tímaáætlanir þeirra. Fyrir utan það, hvernig gætu menn með skrúfjárn framkallað svona kerfisbundið fyrirbæri?"

(þýtt úr *Portrait of Benoit B. Mandelbrot* eftir Monte Davis)



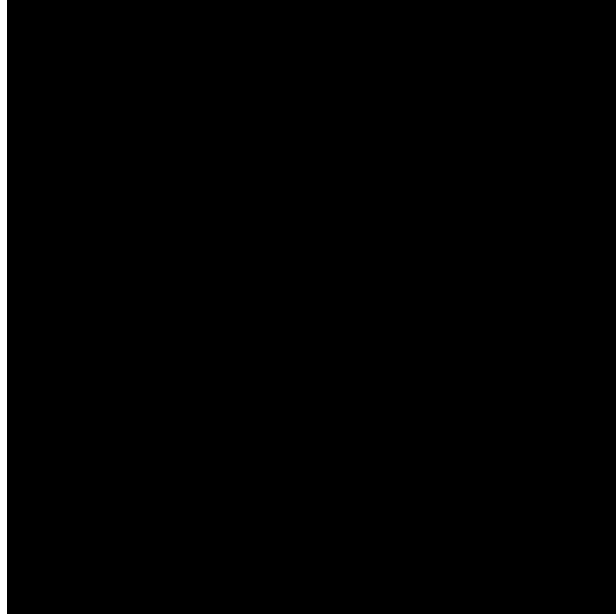
Einföld brotamynd þríhyrnings frá $n=1$ til $n=4$ (Koch Snowflake)

Út frá þessu fór hann að gera tilraunir, og fann út að "hávaði" (e. noise) væri mjög eðlilegt fyrirbæri í náttúrunni, og í raun ógerningur að losna við hann. Eftir að hann hafði fordæmt margar tilraunir til þess að losa sig við hávaðann, þá fór hann að taka eftir einkennilegu röksamhengi í þessu. Þetta samhengi leiddi af sér kenningu um brotmyndarúmfræði (e. fractal geometry), sem að síðan 1975 hefur haft gríðarleg áhrif á það hvernig heimurinn er túlkaður. Ekki einungis hefur þetta gert það auðvelt að líkja eftir þróun lífs í tölvu (*Conways Game of Life*; John Conway, 1970) og jafnvel að búa til flóknar landslagsmyndir út frá mjög einföldum jöfnum. En hvað er brotamynd?

Mandelbrot skilgreindi brotamyndir (e. fractals) þannig: "Brotamynd er beygja þar sem Hausdorff-Besicovitch svigrúm þess er stærri en Evklíðska svigrúm þess". Hausdorff-Besicovitch svigrúmsvídd (oftast kölluð bara eftir fyrri höfund hennar, Felix Hausdorff) er aðferð til þess að reikna nákvæmlega stærðir flókinna gagnasafna á borð við brotamyndir. Hausdorff svigrúmsvíddin gengur alveg eftir hefðbundnum mælingum eðlilegара gagnasetta, en getur reiknað mun flóknari sett og ekki endilega bara náttúrulegar tölur.

Ef að M er þrívítt cartesískt rúm og $d > 0$ er rauntala, þá er d -víða Hausdorff-lengdin $H^d(M)$ skilgreind sem neðra lágmark (e. infimum) allra $m > 0$ þannig að um öll $r > 0$, M gildi að þau séu þekjanleg með teljanlegum fjölda afmarkaðra setta með þvermál $< r$ og summa d -undu veldis af þessum lengdum er minna en eða jafnt og m . (Wikipedia)

Í stuttu máli, þá er Hausdorff-svigrúmsvíddin stærri en Evklíðska svigrúmsvíddin vegna þess að brotamyndin er sífeld endurtekning á sjálfri sér. (Formið er sjálfu sér líkt).



Koch serían

Flokkar brotamynda

Brotamyndum er almennt skipt upp í þrjá flokka: rúmfræðilegar (e. geometric), algebraískar (e. algebraic) og stóatískar (e. stochastic) brotamyndir.

Rúmfræðilegar brotamyndir byggjast upp á einföldum skipulögðum breytingum á n-víðum formum, t.d. brot á reglulegri línu eins og í koch beygjuni hér að ofan.

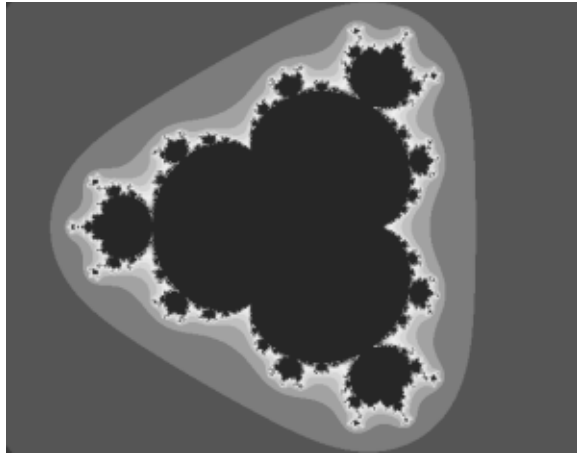
Stóatískar brotamyndir eru búnir til út frá handahófskenndum afleiðum algebraískra brotamynda. Slíkar formúlur eru oft notaðar til þess að búa til upphleypt mynstur, t.d. við kortagerð og veðurfræðiathuganir. Stóatískar brotamyndir eru einnig kallaðar óákveðnar brotamyndir, þar sem að niðurstöður þeirra eru jafn mikið byggðar á gögnunum sem koma inn í fallið og fallinu sjálfu (þ.e., fallið er lang því frá að vera eintækt).

Lang stærsti flokkur brotamynda er þó algebraísku brotamyndirnar. Þeim skiptir hundruðum eða þúsundum, og eru frægustu brotamyndirnar í þeim flokki. Dæmi um brotamyndir í þeim flokki eru Mandelbrot, Mandelbrot⁵, Barnsley₁, Newton og Phoenix. Þær eru langoftast byggðar upp á útreiknuðum endurtekningum á tvinntöluformúlum með mismunandi raunverulega og ímyndaða parta með tilliti til hnitana sem óskað er eftir. Dæmi um þetta væri Mandelbrot⁴ formúlan, sem er þannig:

$$Z_n = Z_{n-1}^4 + C$$

Þar sem að Z og C eru hvorttveggja tvinntölur. Þá er $Z = 0 + 0i = 0$ í fyrstu umferð, og $C = (x/n) + (y/n)i$ þar sem að x og y eru hnitin sem verið er að teikna á hverjum gefnum tíma og n er vísir fyrir það hversu mikla "stækkun" á að vera á brotamyndinni (1 = upprunaleg stærð).

Þá er þessi formúla endurtekin að jafnaði 100 sinnum fyrir hvern punkt og tölugildi punktsins ákvarðaður út frá því. Í dæmigerðum brotamyndahermi er hverju talnagildi gefinn litur sem að nýtist svo til þess að teikna einkar fallega mynd.



Mandelbrot⁴

En þess ber að geta að Mandelbrot settið er tvinntöllumengi þar sem að gildir:

$$x \in \mathbb{C} \mid |x| < 2$$

En það er ekki þar með öllu lokið. Fallegar myndir eru einmitt ekki nema kjarni málsins, en þetta mál vill vinda svolítið upp á sig. Michael F. Barnsley hafði nokkuð gaman af brotamyndum en vildi finna hagnýtt gildi fyrir þær. Þar sem að Barnsley, og vinur hans og samstarfsmaður Alan D. Sloan, hjá Tækniháskólanum í Georgíu hafði verið mikið að vinna með geymslu ljósmynda í tölvutækum gagnasöfnum lét hann sér detta það til hugar að, úr því að allt í náttúrunni virðist samstanda af brotamyndum (e. fractal forms), þá ætti að vera hægt að geyma ljósmynd sem stærðfræðilega lýsingu á mörgum ólíkum brotamyndum. Þeir gerðu nokkrar tilraunir með þetta og árið 1987 höfðu þeir nægileg gögn til þess að geta sótt um einkaleyfi á hugmyndinni. Í þá daga (og enn í dag) var algengasta aðferðin til þess að geyma ljósmyndir á tölvum JPEG ("Joint Photographics Expert Group") staðallinn, sem geymir upplýsingar um hvern einasta punkt í myndinni - hvernig hann er á litinn og hvar hann er staðsettur. Til þess að minnka myndina er notaður mjög einfaldur og vel þekktur þjöppunaralgrímur - strjál kósínus ummyndun (e. discrete cosine transform) - sem tekur alla þá parta myndarinnar sem að eru svipaðir og skellir þeim í einn flokk. Vandinn við JPEG er að það er gæðatap, þrátt fyrir að það sé 90%-95% þjöppun á myndefninu þegar best lætur. Barnsley vildi ekki sætta sig við gæðatap. Hann ályktaði að það væri hægt að nota brotamyndir til þess að geyma upplýsingar um ljósmyndir án gæðataps og án hamla á stærðarhlutföllum, og hann hafði rétt fyrir sér. Hann var hinsvegar alveg var við það að hugmynd hans var ekki neitt lítið afrek, og ákvað að selja þessa tækni frá sér á okurverði, sem leiddi til þess að ókeypis staðlar - þótt óæðri væru - fengu meiri stuðning hjá almenningi.

Brotmyndabjöppun (e. fractal compression) hefur hinsvegar orðið mjög vinsæl hjá stórum fyrirtækjum og stofnunum á borð við NASA sem þurfa að geyma ógrynni gagna á mjög takmörkuðu geymsluplássi. Microsoft keypti leyfi til þess að nota brotmyndabjöppun Barnsleys í Encarta (stafrænu alfræðiorðabókinni), sem er háð þeim stærðartakmörkunum að tugir þúsunda mynda í nær fullkomnum gæðum (það er

minniháttar gæðatap á brotamyndabjöppun) þurfa að rúmast á örfáum geisladiskum.

Augljóst er að hagnýtu notagildi brotamynda eru mörg og misjöfn, og teygja anga sína yfir í gagnabjöppun, rafeindavirkjun, myndlist og ýmislegt fleira. En að okkur vitandi hefur enginn gert tilraunir með notkun þeirra í dulmálsfræðilegum tilgangi.

Kynning á tætişgrímum

Almennt um tætişgríma

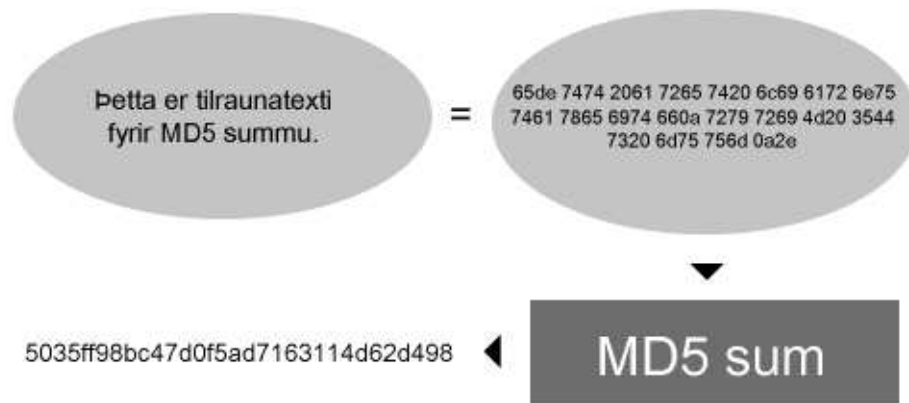
Tætişgrímur (e. hash function) er aðferð til að búa til einkennandi talnastreng úr gögnum. Helsti kostur tætişgríma er sá, ef þeir eru vel hannaðir, er að talnastrengurinn er svo til einstakur, það er að segja; líkurnar á því að sami talnastrengurinn endurtaki sig úr tveimur mismunandi gagnasöfnum eru hverfandi. Einnig ættu tætişgrímar að vera þannig úr garði gerðir að það sé ekki hægt að lesa gögnin úr talnastrengnum sem hann skilar frá sér. Til einföldunar má hugsa sér úrtak tætişgríma sem nokkurskonar fingrafar gagna: það einkennir gögnin án þess að segja hvernig gögnin líta út.

Í upphafi, þegar fyrstu hugmyndirnar um tætişgríma komu fram, var það í þeim tilgangi að sjá til þess að hernaðarlega mikilvæg gögn kæmust rétt til skila og var Alan Turing, faðir tölvunnar, þar fremstur í flokki hugsuða. Eftir seinni heimstyrjöld var Claude Shannon, starfsmaður hjá Bell Labs (nú Lucent Technologies - þar sem transistorinn og besta forritunarmálið sem til er voru þróuð), að velta fyrir sér hvernig upplýsingar hegðuðu sér. Upp úr því lagði hann fram Upplýsingakenninguna (*The mathematical theory of communication*), sem lýsti meðal annars fyrstu þjöppunaraðferðunum, mörgum nothæfum tætişgrímum og stærðfræðilegum takmörkum fyrir hámarksþjöppun upplýsinga án gagnataps. (Shannon, 1948). Einn af fyrstu tætişgrímum var $H(x) = x \bmod(m+1)$ og var sá tætişgrímur trúlega einn af þeim fyrstu til að hljóta almenna viðurkenningu. Tætişgrímar hafa þróast talsvert mikið frá þessum einfalda og fyrirsjáanlega algrími, þeir eru flóknari, hraðvirkari en líka margfalt öruggari.

Tætişgrímar hafa þróast til notkunar á fleiri sviðum en hernaðarlegum, þeir eru notaðir í dulkóðun (til dæmis GnuPG, PGP og OpenSSL) til að auðkenna dulkóðaða textann, til þess að staðfesta innihald gagna (einkum tölvutækra gagna), og margt fleira. Tætişgrímar eru oftast undirliggjandi þar sem þeir eru notaðir og eru notendum þeirra oft ókunnugir. Dæmi um notkun tætişgríma er í ZIP-skjölum sem eru afar algeng nú til dags, en ZIP skjöl eru þjöppuð gagnasöfn sem er þjappað saman með Hoffman þjöppunaralgrímum. Nytsemi tætişgrímana í ZIP skjölum er sá að sjá til þess að innihald gagnasafnana sé rétt eftir afþjöppun þeirra. Tætişgrímar eru líka notaðir í gagnasafnsvinnslu, þar sem bera þarf saman ákveðin gögn við mikið magn annara gagna, þar eru gögnin sjálf geymd í grunninum og fingrafar gagnana einnig, svo þegar þarf að bera saman gögnin við önnur gögn er miðað við fingraför gagnana í staðinn fyrir að miða við gögnin sjálf - þessi aðferð er oft mun hraðvirkari en að bera gögnin sjálf saman.

Tætişgrímar sem notaðir í dag eru fjölmargir, og sem dæmi má nefna SHA1, MD2, MD4, MD5, MDC2 og RIPEMD160. Allir hafa þessir tætişgrímar sína kosti og ókosti, sumir eru óöruggari en aðrir á meðan þeir bæta það upp með meiri hraða. Tveir mest notuðu tætişgrímarnir innan dulkóðunar- og tölvuöryggisheimsins eru SHA1 og MD5. SHA1 var hannaður af *National Security Agency*, í Bandaríkjunum og MD5, sem er enn mikið notaður en talinn óöruggur, var hannaður af *RSA Data Security Inc* í Bandaríkjunum. Þó að þessi nöfn séu vel þekkt og fyrirferðamikil í dulkóðunar- og tölvuöryggisheiminum ber alls ekki að treysta þeim í blindni, þar eð NSA hefur verið

þekkt fyrir persónunjósniir hjá borgurum sínum ásamt því að veikja dulkóðunaralgríma sem þeir hafa búið til til einkanota og RSA hefur mikilla hagsmuna að gæta þar eð algrímar þeirra eru uppspretta peninga. En þó að varast beri að treysta þessum aðilum hafa þeir enga hagsmuni af því að búa til gallaða eða veika tætiigríma, þeir þurfa sjálfir á slíkum algrímum að halda og SHA1 hefur verið skoðaður af óháðum aðilum með áherslu á öryggismál.



Myndræn framsetning á notkun MD5

Þess ber þó að geta að framsetning gagna úr tætiigrímum getur verið mismunandi eftir útfærslu tætiigrímanna í forritum, því geta gögnin hér að ofan verið öðruvísi í öðrum útgáfum af MD5-tætiigrímsforritum.

Stærð gagnana sem tætiigrímar skila frá sér er nefnd blokkarstærð (e. block size), því stærri sem blokkarstærðin er því minni líkur eru á að endurtekningar geti átt sér stað í úttaki tætiigrímsins. Í kjölfar umræðu um SHA1 og MD5 hér að ofan má bæta því við að SHA1 er 160 bitar að blokkarstærð og MD5 128 bitar að blokkarstærð, sem ætti því að ofansögðu að gera SHA1 öruggari en MD5, sem er rétt í öllum meginatriðum. Þetta er þó ekki algilt vegna þess að tætiisalgrímar geta innihaldið galla eða yfirsjónir sem er hægt að finna með miklum og tímafrekum rannsóknum og prufunum á algrímum.

Stærðfræðileg hugmynd tætiigríma

Tætiigrímar vinna þannig að tekin eru gögn, G , í því magni sem fallið $H(x)$ (tætiigrímsfallið $H(x)$) getur tekið við og fyrir hvert stak af gögnum kemur út ákveðin tala sem gengur upp í modúlasummu, sem er þá úttakið úr tætiisalgrímnum. Markmiðið með slíkum algrím er að virka sem einátta reiknirit. Dæmi um þannig fall er Eulers-fí fallið. Gallinn við Eulers fí fallið er þó sá að það skilar ekki frá sér úrtaki sem er einstakt, líkurnar á að fá sama úrtak úr öðru gagnasetti eru miklar og því er Eulers óhæft til raunhæfrar notkunar sem tætiigrímsfall.

Í raun er hægt að nota næstum hvaða fall sem er sem tætiigrímsfall, en þau henta afar misjafnlega til þess brúks og stundum alls ekki.

Nokkur lokaorð um tætiigríma

Tætisgrímar eru nauðsynlegir í allskyns flutningi stafrænna gagna. Þeir búa til fingraför af gögnum og eru send eftir sömu leið og gögnin sjálf eða annari leið, allt eftir aðstæðum og tilefni, og eru notuð til að athuga hvort að gögnin komust rétt til skila. Tætisgrímar eru nauðsynlegir vegna þess að sitthvað getur farið úrskeiðis í stafrænum gagnaflutningi, en galdurinn er sá að senda gögnin aftur ef eitthvað fór úrskeiðis í stað þess að reiða sig á gögn sem eru mögulega skemmd.

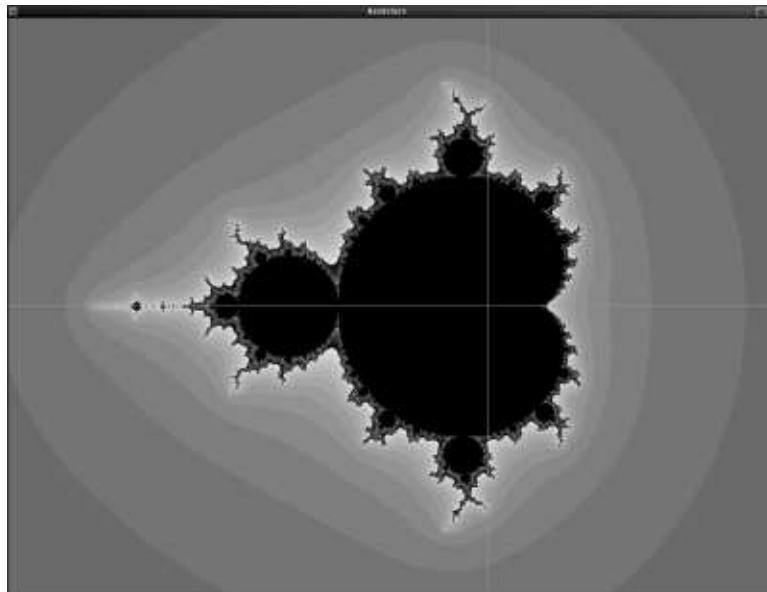
Framkvæmd athuganna og niðurstöður

FractalGen forritið

Til þess að geta betur áttað okkur á hegðun brotamynda ákváðum við að byrja á því að forrita einfaldan Mandelbrot hermi. Hann vann bara út frá $Z_n = Z_{n-1}^2 + C$ (Mandelbrot²) jöfnunni með tvinntöluna $C = x + yi$, þar sem að x og y voru hnit punktsins sem átti að teikna hverju sinni. Forritið gaf góða raun og gátum við séð þá marglitt á svörtu hvernig brotamyndin hegðaði sér við hinar ýmsu aðstæður. Út frá þessu unnum við nokkrar aðrar brotamyndir með því að fíkta í jöfnunni - að prófa hinar ýmsu samsetningar tvinntalna í hinum ýmsu veldum. Þar sem að við höfðum ekki til umráða aðgerðasafn fyrir tvinntölur urðum við að handreikna þær þannig að hvort raunverulegi og ímyndaði partur tvinntalnanna var höndlaður alveg út af fyrir sig nema að nauðsynlegt væri að höndla þær saman. Þá skilgreindum við:

```
double cr = 0.3 * ((x+xpan+zoomx)/zoomfactor);  
double ci = 0.3 * ((y+ypan+zoomy)/zoomfactor);
```

Þannig að cr er raunverulegi partur C , og ci er ímyndaði partur hennar. x og y táknuðu þá hnitin sem átti að vinna út frá, og $xpan$, $ypan$, $zoomx$, $zoomy$ voru skilgreindir fastar sem virkuðu til þess að jafna myndina betur út á miðju skjásins, okkur til þæginda við könnun brotamyndarinnar. Þá var $zoomfactor$ tala sem við breyttum eftir hentisemi til þess að stækka myndina upp á vissum köflum til þess að skoða myndina nánar.



Skjámynd af FractalGen forritinu

Þá skilgreindum við tvinntöluna Z sem tvær double (fleytitölu) breytur, zr og zi . Þær voru báðar núllstilltar í upphafi. Síðan skilgreindum við fleytitölubreytuna t , en hún verður notuð í lykkjunni. Þegar þessu var lokið hófst ferlið sem við lýsum hér í hálfkóða:

```

byrja endurtekningu:
  á meðan (n < 100) ^ ((zr2 + zi2) < 100):
    n := n + 1;
    t := zr2 - zi2 + cr;
    zi := 2*zr*zi + ci;
    zr := t;
endur;

```

Áð þessu loknu var talan n á bilinu 0 til 100. Þá gáfum við hverri tölu á þessu bili litagildi, þar sem að 100 = svartur, og teiknuðum punkt í þeim lit á punktinn (x,y) . Þetta ferli er endurtekið fyrir hvern einasta punkt á skjánum.

m2h forritið

Þegar að við höfðum kynnst Mandelbrot ágætlega ákváðum við að nú væri mál að nýta jöfnuna til góðs málefnis. Við bjuggum til nýtt forrit sem að vann út frá því að um Mandelbrot² mynd væri að ræða, og tók inn gögn úr inntaksskjalinu í pörum. Ef að ekki væri fullnægjandi magn gagna í inntaksskjalinu til þess að fylla bæði pörin, þá var sett núll í staðinn. Gagnapörin, $P = (x,y)$, þar sem að x og y eru 16 bita heiltölur, eru lesnar úr skránni í MSB (Most Significant Byte first) röð, og er þá textinn "YBVL" samsvarandi tölugildinu $4C564259_{hex} = 1280721497_{tug}$. Það væri þá lesið í hnit þannig að

$$P = (4C56_{hex}, 4259_{hex}) = (19542, 16985)$$

Þá væru þau hnit keyrð í gegnum reikniritið sem við bjuggum til í FractalGen forritinu, og fengin út tölulegt gildi fyrir þau á milli 0 og 100. Sú tala var þá lögð saman við 128 bita summuna eftir ákveðnu ferli sem lýst er hér með C kóða:

```

while(!feof(fp)) {
  fread(&x, 4, 1, fp);
  fread(&y, 4, 1, fp);
  hash[count % (HASH_LENGTH+1)] += ((mandelbrot(x, y) << r) * mandelbrot(y, x));
  count++;
  r++;
  if (r > 24) {
    r = 0;
  }
}

```

Þar sem að HASH_LENGTH er skilgreint sem 4, og hash er fylki af HASH_LENGTH mörgum 32 bita tölum.

$4 * 32 = 128$ bit, sem að er lengdin sem við ákváðum að hafa á tæti fallinu. Þar sem að C býður ekki upp á að vinna með stærri tölur en 32 bit í einu, þá urðum við að búa til fylki og vinna með þetta búi fyrir búi. Þá er "count % (HASH_LENGTH+1)" samsvarandi

$c \bmod(5)$, þar sem $c = \text{count}$. Þá erum við að hafa áhrif á mismunandi parta fylkisins í hverri umferð. Þetta gerum við til þess að auka fjölbreytnina í útkomu tætifallsins. Þá leggur forritið við mengið töluna sem er fengin úr brotamyndinni og færð til vinstri um r sæti (miðað við tvenndarkóða), þar sem að r er tala milli 0 og 24 til þess að færa 8 bita töluna á bilinu 0 til 100 mest til um $32 - 8 = 24$ sæti, og svo margfölduð með útkomunni úr brotamyndinni aftur (nema með víxluðum hnitum). Þetta er allt gert til þess að auka fjölbreytnina á niðurstöðunum.

Að þessu loknu hefur forritið lokið keyrslu sinni. Það skrifar svargildi tætifallsins út á skjáinn og hættir.

Til þess að prufukeyra þetta keyrðum við forritið á nokkrar misjafnlega stórar skrár. Fengum við þá nokkuð skemmtilegar niðurstöður fyrst um sinn:

323ddee0b547d91013b0b4142f2b98d6	Spaceballs.avi
81ca8a00f06b9600d5dbd6c8edc9b78a	hitchhiker's guide - part 9.mp3

En svo þegar að við byrjuðum að skoða minni skrár, þá komu gallarnir í ljós: Séu tvær mismunandi skrár búnar til, sem dæmi; önnur samanstendur einungis af strengnum AAAA og hin af AAAB og forritið keyrt á þessar skrár kemur út sama úttakið. Þetta er stór galli sem orsakast af því að tölugildin á A og B eru mjög lík - A hefur 1 lægra gildi en B - og staðsetning A og B eru á svipuðum slóðum í mandelbrotmyndinni og kemur því út sama úrkoma úr mandelbrot fallinu. Þetta útskýrir sama úttak úr forritinu okkar.

Á hinn bóginn er ekki hægt að lesa úr úttaki forritsins gögnin sem voru lögð til grundavallar úttakinu, því er stöðugt breytt á keyrsluferlinu og það vantar hreinlega meiri gögn til að geta lesið inntakið úr úttakinu.

Niðurstöður

Mandelbrot² er ekki nothæf brotamynd til öruggrar notkunar sem tætisgrímur. Að þessari niðurstöðu liggja þau rök að tætisgrímur sem á að vera öruggur má ekki skila sama úttaki á tveimur ólíkum gagnasöfnum, eða að minnsta kosti eiga líkurnar að vera mjög litlar á að slíkt gerist. Svo er ekki með forritið okkar, eins og hægt er að lesa af dæminu að ofan. En hins vegar á tætisgrímur líka að vera þannig að ekki sé hægt að lesa úr úttakinu hvaða gögn voru lögð til grundvallar þess, það er í góðu lagi í forritinu okkar. Mjög líklega væri hægt að nota fjölbreyttari brotamynd, til dæmis Barnsley 1 formúluna, í meiri stækkun og hliðrun, til þess að fá ófyrirsjáanlegari niðurstöður. Það væri ef til vill líka sniðugt að nota línulega "brotamynd" og höndla gagnasettið ekki sem töluleg hnit heldur sem einvíðan vigur út frá síðasta punkti. En þó teljum við að lang sterkasti leikurinn væri að gera tilraunir með notkun stóatískra brotamynda. Þar sem að þær eru byggðar á handahófskenndum afleiðum algebrískra falla væri hægt að reyna að finna fyrirsjáanlega runu í ólínulegu stóatísku falli og beita því til þess að fá mjög sértækar niðurstöður. Einnig væri ráð að beita fleiri aðferðum til þess að tryggja fjölbreytni fingrafarsins, til dæmis að "rúlla" tvenndarstrengnum upp um sjálfan sig. Það er, að strengurinn 10011_{bin} væri rúllaður um $10011_{\text{bin}} = 19$, þannig að hann yrði 110001_{bin} eftir 19 vinstri rúllur (ROTL - vinstri rúlla, er svipuð og vinstri hliðrun, nema það að ef að bit "dettur fram af" byte-boundryinu, 8. sætisgildið, þá birtist það í fyrsta sætisgildinu í

stað þess að það sé fyllt með núlli.).

Þrátt fyrir að tilraun okkar hafi ef til vill ekki getið af sér nothæft tætifall teljum við að það sé mjög auðvelt að búa til tætiföll út frá brotamyndum með viðunandi árangri. Það er alveg augljóst að þessi meðferð tvinntalna er tölvum ekki jafn hægur leikur að vinna með og modúlus vinnslan sem er algengust í tætiföllum, en þó virðist hún koma sterk inn með hliðsjón af tilraunum ýmissa fyrirtækja við notkun á glundroðakenningu (e. chaos theory) í dulkóðunartilgangi, en þar er Bodacions ef til vill frægasta dulmálið. Þar sem að brotamyndum fylgir ákveðinn fyrirsjáanlegur grundroði - þar sem að þetta eru náttúruleg fyrirbrigði að mestu - þá er hægt að sjá fleiri mögulegar útkomur úr einu slíku falli en í mörgum hefðbundnum föllum. Náttúran sér um alla erfiðisvinnuna.

Hefnd koffeinsins

Margt býr í kýrhausnum sagði einhver vitur maður einhverntímann. Ef til vill mætti líkja þessari ritgerð við kýrhaus; efni hennar spannar nokkuð mörg svið stærðfræðinnar: tvinntölur, stóatísk rúmfræði, upplýsingakenningu Shannons, Hoffmann-þjöppun, dulmálfræði og fleira til.

Við notuðum okkar eigin áhugasvið, okkar eigin þekkingu og þekkingu sem við sóttum úr ýmsum áttum og úr varð þessi líka fíni kokteill: ritgerð um notkun brotamynda í tættisgrímum. Við lærðum helling á þessu ævintýri og jafnframt áttum við ágætar stundir við að dunda við smíði á ritgerðinni ásamt því að prufa ýmislegt og leika okkur. Við lærðum jú alltént það að notkun brotamynda í tættisgrímum er alls ekki svo fráleit hugmynd þó að við getum ekki notað Mandelbrot² þannig. Gaman væri að prufa fleiri gerðir brotamynda í framtíðinni, en það verður að bíða betri tíma.

Vestmannaeyjum 19. Maí 2003,

Smári P. McCarthy,
Guðmundur D: Haraldsson.

Heimildir

The mathematical theory of communication

Claude Shannon, Bell Labs, 1948.

Interactive Computer Graphics, second edition

Edward Angel, Addison-Wesley, New York, 2000.

Mandelbrot. - Benoit Mandelbrot. 17. Maí 2003. <http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Mandelbrot.html>

Shannon - Claude Elwood Shannon. 17. Maí 2003. <http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Shannon.html>

Julia - Gaston Maurice Julia. 17. Maí 2003. <http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Julia.html>

An Introduction to Cryptography 8.0.

PGP Corporation, 2002.

Hausdorff-Besicovitch Dimension

http://www.weihenstephan.de/ane/dimensions/subsection3_3_4.html

Mathworld

<http://mathworld.wolfram.com/>

Wikipedia

http://www.wikipedia.org/wiki/Hausdorff_dimension

Stochastic fractals

<http://www.aci.net/kalliste/StochFrac.html>

Benoit Mandelbrot, Fractals and Astronomy

<http://www.umich.edu/~lowbrows/reflections/1998/dsnyder.3.html>