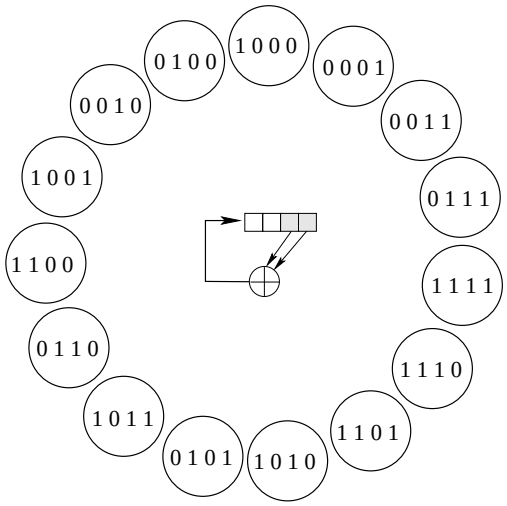
LFSR

Aleksandar Jurišić

20. april 2008

V nalogi o pinih smo sešteli vse števke. Lahko pa bi sešteli le nekatere izmed njih. Tovrstna posplošitev nas pripelje do praktičnih objektov. LFSR je kratica za linear feedback shift register, tj. *linearni povratni pomični register*.



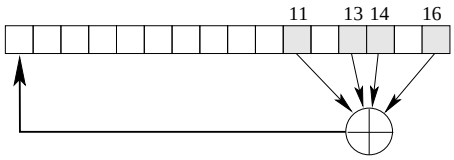
Slika 1: 4-bitni LFSR z diagramom stanj. Maksimalno zaporedje sestavljamo vsa možna stanja z izjemo "0000".

Opišemo ga lahko kot zaporedje registrov, ki so postavljeni v vrsto in vsebujejo bitne vrednosti. Pravimo jim *stanje* (v naši nalogi pa je stanje predstavljal PIN). Na vsakem koraku se stanje spremeni na naslednji način. Vrednosti zamaknemo za eno mesto, tisto, ki pade ven pozabimo ali kam zapišemo za kasnejšo uporabo, na prazno mesto pa vstavimo nov bit, ki ga izračunamo z linearno funkcijo iz prejšnjega stanja. Edina linearna funkcija enega samega bita je XOR ali inverzni XOR, kar pomeni, da gre za pomični register, katerega vhodni bit izračunamo z XOR-om nekaterih bitov iz stanja.

Začetno stanje LFSR-ja imenujemo *seme*. Ker so vse operacije deterministične, je zaporedje bitov, ki jih dobimo popolnoma določeno iz tekočega (ali kakšnega predhodnega) stanja. Vsak register ima končno število možnih stanj (bolj natančno 2^n, kjer je n dolžina registra), zato se čez čas vrednosti začnejo periodično ponavljati. Temu pravimo, da so se vrednosti zaciklale. Vendar lahko te vrednosti pri skrbno izbrani povratni funkciji izgledajo precej naključne, cikel pa je izredno dolg.

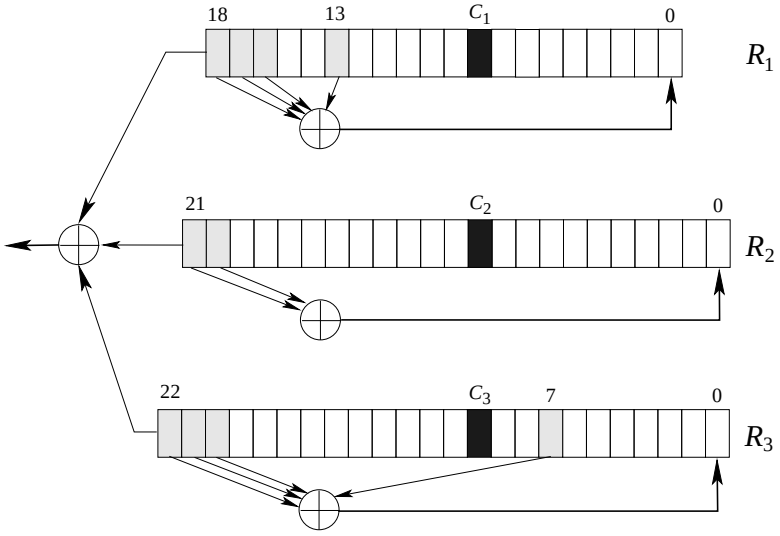
Pogoste so implementacije tako v programski opremi kakor v strojni opremi. LFSR-ji so tako-rekoč nepogrešljivi pri konstrukciji hitrih psevdo-naključnih zaporedij.

Izhodno zaporedje bitov oziroma stanja lahko računamo tudi v obratni smeri, tako da za začetno zaporedje vzamemo zrcalno sliko originalnega začetnega zaporedja.



Slika 2: 16-bitni Fibonaccijev LFSR.

LFSR se uporablja na različnih področjih, npr. GPS (Global Positioning System) za hitro prenašanje zaporedij, ali pa pri video igrah (Nintendo Entertainment System) kot sestavni del ozvočenja. Na LFSR temeljijo tudi različne tokovne šifre, kot so A5/1, A5/2, E0,. . . , vendar pa bi se morali tu spustiti v tehnične podrobnosti in se zadovoljimo z vabilom, ki ga predstavlja naslednja slika.



Slika 3: A5/2