به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۸ اسفند ۹۲

جلسه‌ی ۷: ثبات خطی و رمزهای دنباله‌ای

مدرس: دکتر شهرام خزائی *نگارنده: افشین زارعی، مهدی جعفرنیای جهرمی*

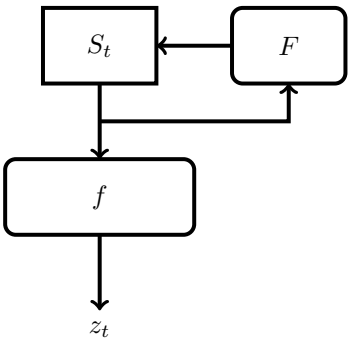
در جلسه قبل، مولد شبه‌تصادفی که یک کلید اولیه با طول کوچک تصادفی را به یک دنباله طولانی‌تر تبدیل می‌کند، معرفی شد. در این جلسه، LFSR به عنوان یک پیشنهاد اولیه برای مولد شبه‌تصادفی معرفی می‌شود. اما به دلایلی که خواهیم دید، مولد حاصل را نمی‌توان یک مولد شبه‌تصادفی امن در نظر گرفت. در این جلسه ابتدا روش کلی طراحی مولد شبه‌تصادفی و سپس ویژگی‌های LFSR معرفی می‌شود. در جلسه‌ی آینده نحوه‌ی استفاده از LFSR برای ساختن مولدهای شبه‌تصادفی امن را خواهیم دید.

۱ روش کلی طراحی مولد شبه‌تصادفی

مولدهای شبه‌تصادفی اصطلاحاً رمز دنباله‌ای نیز نامیده می‌شوند و به دنباله خروجی آنها جریان‌کلید[۱] یا کلید اجرایی[۲] گفته می‌شود. به طور کلی یک رمز دنباله‌ای را می‌توان به شورت یک ماشین حالت محدود[۳] طراحی کرد که حالت اولیه‌ی آن به کلید وابسته است. یک ماشین حالت محدود به صورت زیر قابل تعریف است:

$$S_t = F(S_{t-1}), \quad t \geq 1$$
$$z_t = f(S_t), \quad t \geq 1$$

که در آن $F : \mathbb{F}_2^L \to \mathbb{F}_2^L$ تابعی است که یک حالت را (که با L بیت مشخص می‌شود) به حالت بعدی تبدیل می‌کند و $f : \mathbb{F}_2^L \to \mathbb{F}_2$ تابعی است که با دریافت یک حالت به عنوان ورودی یک بیت را به عنوان خروجی پس می‌دهد. توجه کنید که $S_t = (s_{t,0}, s_{t,1}, ..., s_{t,L-1})^T$ بردار حالت در زمان t است و $S_0 = (s_{0,0}, s_{0,1}, ..., s_{0,L-1})^T$ بردار حالت اولیه است و z_t بیت کلید اجرایی در زمان t است. بدین ترتیب می‌توان روش کلی طراحی مولد شبه‌تصادفی را در شکل زیر نشان داد.



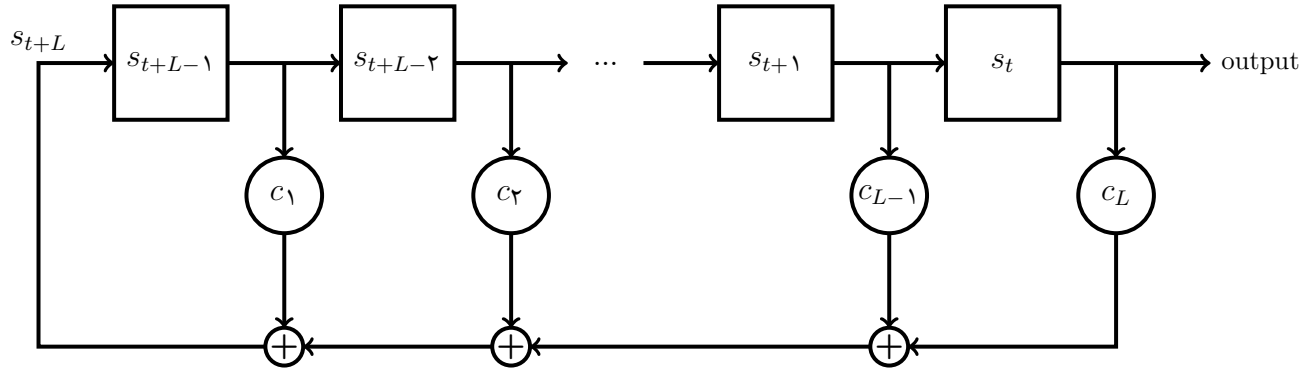
[۱] keystream
[۲] running-key
[۳] finite-state machine

۲ ثبات با بازخورد خطی

یک ثبات با بازخورد خطی[۴] (LFSR) با استفاده از چندجمله‌ای بازخورد[۵] $C(X) = ۱ - \sum_{i=۰}^{L} c_i X^i \in \mathbb{F}_q[X]$ تعریف می‌شود که L طول ثبات نامیده می‌شود. این ثبات رشته‌ی $(s_۰, s_۱, \cdots, s_{L-۱}) \in \mathbb{F}_q^L$ را (که حالت اولیه نامیده می‌شود) با استفاده از رابطه‌ی بازگشتی زیر به یک دنباله با طول نامتناهی تبدیل می‌کند.

$$\forall t \geq ۰ \ ، \ s_{t+L} = \sum_{i=۱}^{L} c_i s_{t+L-i}$$

در این صورت دنباله‌ی خروجی یک LFSR بصورت $(s_t)_{t\geq ۰}$ است.
در شکل زیر روند کار یک LFSR به طول L را می‌بینید.



۱.۲ چندجمله‌ای بازخورد و چندجمله‌ای مشخصه

دنباله‌ی خروجی یک LFSR بصورت یکتایی بوسیله ضرایب چندجمله‌ای بازخورد و حالت اولیه تعیین می‌شود. ضرایب بازخورد $c_۱, c_۲, \cdots, c_L$ یک LFSR با طول L بوسیله‌ی چندجمله‌ای بازخورد که بصورت زیر تعریف می‌شود، مشخص می‌شوند.

$$C(X) = ۱ - \sum_{i=۱}^{L} c_i X^i.$$

همچنین این ضرایب را با استفاده از چندجمله‌ای مشخصه[۶] می‌توان بدست آورد:

$$C^*(X) = X^L C(\frac{۱}{X}) = X^L - \sum_{i=۱}^{L} c_i X^{L-i}.$$

[۴] Linear Feedback Shift Register
[۵] feedback polynomial
[۶] characteristic polynomial

مثال ۱ *برای یک $LFSR$ با طول ۴ در میدان $\mathbb{F}_۲$ و ضرایب بازخورد $c_۱ = c_۲ = ۰, c_۳ = c_۴ = ۱$، چندجمله‌ای بازخورد و چندجمله‌ای مشخصه به ترتیب بصورت*

$$C(X) = ۱ + X^۳ + X^۴ \in \mathbb{F}_۲[X]$$

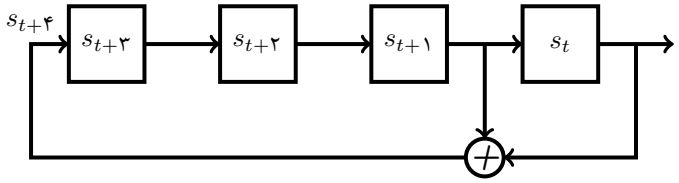
و

$$C^*(X) = ۱ + X + X^۴ \in \mathbb{F}_۲[X]$$

است.
دنباله‌ی خروجی این $LFSR$ با توجه به رابطه بازگشتی زیر تعیین می‌شود.

$$s_{t+۴} = s_t + s_{t+۱} \mod ۲$$

در شکل زیر روند تولید این دنباله را می‌بینید.



برای مثال اگر حالت اولیه را برابر $(s_۰, s_۱, s_۲, s_۳) = (۱, ۰, ۱, ۱)$ قرار دهیم، طبق جدول زیر دنباله‌ی خروجی تولید می‌شود.

t	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
s_t	۱	۰	۱	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱
$s_{t+۱}$	۰	۱	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱	۰
$s_{t+۲}$	۱	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱	۰	۱
$s_{t+۳}$	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱	۰	۱	۱

دنباله‌ی $(s_t)_{t\geq ۰}$ متناوب نامیده می‌شود اگر عدد صحیحی چون T باشد وجود داشته باشد بطوری‌که برای هر $t \geq ۰$ داشته باشیم $s_t = s_{t+T}$. کوچکترین عدد صحیحی که برای آن رابطه فوق برقرار باشد دوره‌ی تناوب دنباله نامیده می‌شود.

تعریف ۲ *یک $LFSR$ را غیرتکین گوییم، هرگاه در چندجمله‌ای مشخصه c_L غیر صفر باشد.*

یک LFSR با طول L روی $\mathbb{F}_q$ دارای q^L حالت مختلف است که حالت تمام صفر همواره به خودش انتقال می‌یابد. دنباله خروجی هر LFSR غیرتکین با طول L روی $\mathbb{F}_q$ متناوب است و دوره‌ی تناوب آن حداکثر $q^L - ۱$ است، یعنی بعد از حداکثر $q^L - ۱$ بار اجرای LFSR به حالت اولیه می‌رسیم.

تعریف ۳ *مرتبه‌ی چندجمله‌ای $C(X)$ برابر کوچکترین عدد صحیح و مثبت T است که $C(X) \mid (۱ - X^T)$.*

برای هر چندجمله‌ای غیرتکین $C(X) \in \mathbb{F}_q[X]$ با درجه L همواره داریم $C(X) \mid (۱ - X^{q^L - ۱})$؛ لذا $T \leq q^L - ۱$.
یک روش برای بدست آوردن مرتبه‌ی چندجمله‌ای $C(X)$ استفاده از روش تقسیم طولانی است. به این صورت که چندجمله‌ای ۱ را به چندجمله‌ای $C(X)$ تا زمانی که باقیمانده برابر X^T شود، تقسیم می‌کنیم (در میدان $\mathbb{F}_q$)؛ یعنی $\frac{۱}{C(X)} = Q(X) + \frac{X^T}{C(X)}$، در این صورت مرتبه‌ی چندجمله‌ای $C(X)$ برابر T است. البته الگوریتم‌های کاراتری نیز برای محاسبه مرتبه‌ی چندجمله‌ای‌ها وجود دارد.

تعریف ۴ *چندجمله‌ای $P(X) \in \mathbb{F}_q[X]$ تحویل‌ناپذیر نامیده می‌شود اگر نتوان آنرا روی $\mathbb{F}_q[X]$ به صورت حاصل‌ضرب دو چندجمله‌ای با درجه کمتر نوشت. یک چندجمله‌ای تحویل‌ناپذیر درجه‌ی L روی $\mathbb{F}_q[X]$ را اولیه[۷] گوییم، هرگاه مرتبه‌ی آن $q^L - ۱$ باشد.*

[۷] primitive

قضیه ۱ *اگر $(s_t)_{t\geq 0}$ دنباله‌ی تولید شده بوسیله‌ی یک $LFSR$ به طول L با چندجمله‌ای بازخورد تحویل‌ناپذیر $C(X) \in \mathbb{F}_q[X]$ از یک حالت اولیه تمام ناصفر باشد، آنگاه دوره تناوب دنباله $(s_t)_{t\geq 0}$ با مرتبه‌ی چندجمله‌ای $C(X)$ برابر است.*

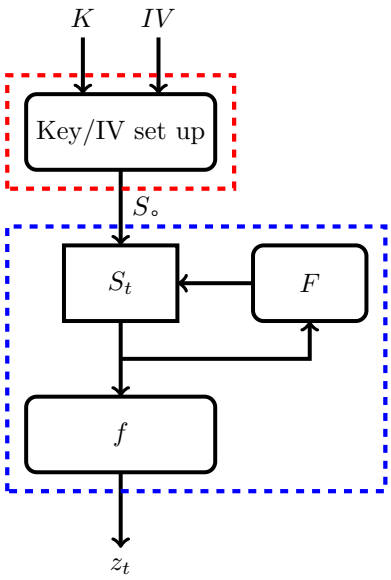
نتیجه ۵ *دنباله خروجی هر $LFSR$ با طول L و چندجمله‌ای بازخورد اولیه روی $\mathbb{F}_q$ از هر حالت اولیه تمام ناصفر دارای دوره‌ی تناوب $q^L - 1$ است. به‌علاوه، تمام حالت‌های تمام ناصفر در هر دوره دقیقاً یک‌بار ظاهر می‌شوند.*

لم ۲ *اگر $(s_t)_{t\geq 0}$ دنباله‌ی تولید شده بوسیله‌ی یک $LFSR$ به طول L با چندجمله‌ای بازخورد تحویل‌ناپذیر $C(X) \in \mathbb{F}_q[X]$ از یک حالت اولیه تمام ناصفر باشد، آنگاه این دنباله توسط هیچ $LFSR$ با طول کمتر از L تولید نمی‌شود.*

در جلسه‌ی آینده خواهیم دید که ویژگی خطی LFSR باعث می‌شود که نتوان از آن به عنوان یک مولد شبه‌تصادفی امن استفاده کرد. به علاوه بررسی خواهیم کرد که چه تغییراتی را باید اعمال کنیم که بتوانیم با استفاده از آن مولد شبه‌تصادفی امن بسازیم.

۳ رمزهای دنباله‌ای مدرن

همانگونه که قبلاً مطرح شد، از خروجی مولد شبه‌تصادفی به جای کلید کاملاً تصادفی در سیستم رمز یک‌بار مصرف (OTP) استفاده می‌شود. استفاده از مولد شبه‌تصادفی به این صورت محدودیت اصلی OTP را داراست؛ یعنی، از هر کلید فقط یکبار برای رمز کردن یک پیام که طولش حداکثر برابر طول دنباله خروجی مولد است می‌توان استفاده کرد. برای رفع این مشکل، رمزهای دنباله‌ای مدرن علاوه بر کلید K از یک مقدار اولیه[۸] IV هم استفاده می‌کنند. با استفاده از الگوریتم بارگذاری کلید[۹] (یا آغازسازی[۱۰])، ابتدا کلید و مقدار اولیه به یک حالت اولیه نگاشته می‌شود و سپس با استفاده از مولد شبه‌تصادفی به یک دنباله طولانی شبه‌تصادفی تبدیل می‌شود. شمای کلی طراحی یک رمز دنباله‌ای مدرن در شکل زیر نشان داده شده‌است.



[۸] Initial Value
[۹] Key/IV setup
[۱۰] initialization

مقدار اولیه معمولاً عمومی است و به همراه متن رمزی ارسال می‌شود. بدین ترتیب هرچند که کلید در طول الگوریتم رمزنگاری ثابت است، اما تغییر مقدار اولیه باعث می‌شود که دنباله‌کلید خروجی نیز تغییر کند و بتوان از یک کلید برای رمز کردن چندین پیام استفاده کرد. در واقع با این روش به کمک مولد شبه‌تصادفی یک تابع شبه‌تصادفی[۱۱] ساخته‌ایم که مقدار اولیه را به عنوان ورودی می‌گیرد و یک رشته را به عنوان خروجی پس می‌دهد. در ادامه درس در مورد توابع شبه‌تصادفی و کاربردهای آن‌ها صحبت خواهیم کرد.

[۱۱] pseudorandom function

به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۸ اسفند ۹۱

جلسه‌ی هفتم: جبر مقدماتی، ریاضیات ثبات خطی

مدرس: دکتر شهرام خزائی *نگارنده: افشین زارعی*

۱ آشنایی مقدماتی با گروه، حلقه و میدان

۱.۱ گروه

تعریف ۱ *مجموعه‌ی G به همراه عمل دوتایی $*$ را که دارای شرایط زیر است، گروه می‌نامیم و با دوتایی $(G,*)$ نمایش نشان می‌دهیم:*

۱. *بسته بودن*

$$\forall a,b \in G : a*b \in G$$

۲. *شرکت‌پذیری*

$$\forall a,b,c \in G : (a*b)*c = a*(b*c)$$

۳. *عضو همانی*

$$\exists e \in G \, \forall a \in G : a*e = e*a = a$$

۴. *عضو معکوس*

$$\forall a \in G \, \exists a^{-1} \in G : a*a^{-1} = a^{-1}*a = e$$

تعریف ۲ *گروه $(G,*)$ را جابجایی (آبلی) گوییم هرگاه: $\forall a,b \in G : a*b = b*a$.*

مثال ۳ *دوتایی $(\mathbb{Z}_2,+)$ که $\mathbb{Z}_2 = \{0,1\}$ و عمل $+$ همان عمل جمع در مبنای ۲ است، یک گروه است.*

مثال ۴ *بطور کلی اگر n عدد طبیعی بزرگتر از یک باشد، $(\mathbb{Z}_n,+)$ یک گروه است (عمل گروه جمع در مبنای n است).*

۲.۱ حلقه

تعریف ۵ *مجموعه‌ی R همراه با دو عمل دوتایی $+$ و $*$ را حلقه می‌نامیم و با سه‌تایی $(R,+,*)$ نمایش می‌دهیم، هر گاه دارای خواص زیر باشد:*

۱. *$(R,+)$ یک گروه آبلی باشد.*

۲. *نسبت به عمل دوم بسته باشد.*

$$\forall a,b \in R : a*b \in R$$

۳. *نسبت به عمل دوم شرکت‌پذیر باشد.*

$$\forall a,b,c \in R : (a*b)*c = a*(b*c)$$

۴. *توزیع‌پذیری عمل دوم نسبت به عمل اول از چپ و راست:*

$$\forall a,b,c \in R : (a+b)*c = (a*c)+(b*c)\ ,\ a*(b+c) = (a*b)+(a*c)$$

مثال ۶ *مجموعه‌ی اعداد صحیح همراه با جمع وضرب معمولی یک حلقه است که با* $(\mathbb{Z},+,\times)$ *نشان می‌دهند.*

مثال ۷ *مجموعه‌ی اعداد حقیقی همراه با جمع و ضرب معمولی یک حلقه است که با* $(\mathbb{R},+,\times)$ *نشان می‌دهند.*

۳.۱ میدان

تعریف ۸ *حلقه‌ی* $(F,+,*)$ *را میدان می‌نامیم، هرگاه* $(F^*,*)$ *نیز یک گروه آبلی باشد (منظور از* F^* *مجموعه‌ی* $F-\{۰\}$ *است، که* ۰ *عضو خنثی عمل* $+$ *است).*

مثال ۹ $(\mathbb{R},+,\times)$ *یک میدان است ولی* $(\mathbb{Z},+,\times)$ *میدان نیست.*

نکته ۱ *میدان متناهی* q *عضوی را با* $\mathbb{F}_q$ *نشان می‌دهیم. تعداد اعضای هر میدان متناهی توانی از عددی اول است؛ یعنی،* $q=p^n$ *به‌ازای یک عدد طبیعی* n *و یک عدد اول* p*.*

نکته ۲ *کوچکترین میدان:* $(\mathbb{F}_۲,+,\cdot)$ *که* $\mathbb{F}_۲ = \{۰,۱\}$ (۰ *عضو خنثی عمل* $+$ *و* ۱ *عضو خنثی عمل* $\cdot$ *است).*

۴.۱ چند حلقه‌ی مفید

حلقه‌ی چندجمله‌ای‌ها: اگر F میدان باشد، $(F[X],+,\cdot)$ را حلقه‌ی چندجمله‌ای‌ها می‌نامیم و به صورت زیر تعریف می‌شود:

$$F[X] = \{a_۰ + a_۱X + \ldots + a_nX^n | a_i \in F\}$$

در حلقه‌ی چندجمله‌ای‌ها تنها عناصر وارون‌پذیر ثابت‌ها (a_i) هستند.

حلقه‌ی سری‌های توانی: بیاد بیاورید که تابع $a:\mathbb{N}_۰ \longrightarrow F$ (که $\mathbb{N}_۰ = \mathbb{N}\cup\{۰\}$) یک دنباله نامیده می‌شود، که معمولاً به صورت $a_۰,a_۱,a_۲,\cdots$ نمایش داده‌می‌شود.
فرض کنید F یک میدان باشد و $F[[X]]$ مجموعه‌ی تمام دنباله‌ها از عناصر مانند $(a_۰,a_۱,\cdots)$ از عناصر F باشند. $F[[X]]$ با جمع و ضربی که به صورت زیر تعریف شده‌اند یک حلقه است که به آن حلقه‌ی سری توانی روی میدان F می‌گویند.

$$(a_۰,a_۱,a_۲,\cdots)+(b_۰,b_۱,b_۲,\cdots) = (a_۰+b_۰, a_۱+b_۱,, a_۲+b_۲,\cdots)$$

و

$$(a_۰,a_۱,a_۲,\cdots)\cdot(b_۰,b_۱,b_۲,\cdots) = (c_۰,c_۱,c_۲,\cdots)$$

که

$$c_n = \sum_{i=۰}^{n} a_ib_{n-i}$$

چندجمله‌ای مولد[۱] دنباله $(a_۰,a_۱,a_۲,\cdots)$ که به بصورت زیر تعریف می‌شود روش دیگری برای نمایش دنباله‌ها است:

$$A(X) = a_۰ + a_۱X + a_۲X^۲ + \cdots = \sum_{k=۰}^{\infty} a_kX^k.$$

[۱] generating function

چندجمله‌ای مولد حاصل‌جمع (حاصل‌ضرب) دو دنباله همان حاصل‌جمع (حاصل‌ضرب) چندجمله‌ای‌های مولد دنباله است. لذا حلقه‌ی سری توانی روی میدان F را بصورت $F[[X]] = \{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in F\}$ نیز نمایش می‌دهند.

نکته ۳ *در حلقه سری‌های توانی تنها چندجمله‌ای‌های غیرتکین $A(X)$ (یعنی $A(0) \neq 0$ یا معادلاً $a_0 \neq 0$) معکوس‌پذیرند. زیرا اگر $A(X) = a_0(1 - B(X))$ که $B(X)$ یک چندجمله‌ای تکین است (یعنی $B(0) = 0$) در اینصورت داریم:*

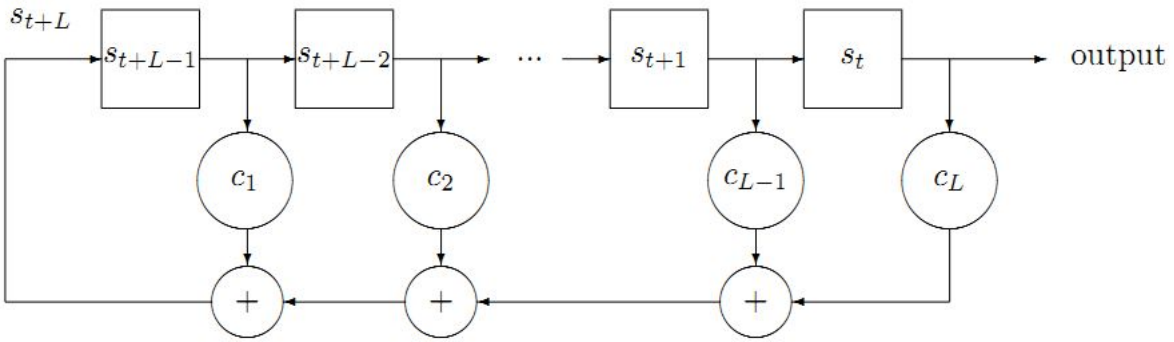
$$A(X)^{-1} = \frac{1}{A(X)} = \frac{1}{a_0(1 - B(X))} = a_0^{-1}(1 + B(X) + B(X)^2 + \ldots) = a_0^{-1} \sum_{k=0}^{\infty} B(X)^k$$

۲ ثبات با بازخورد خطی

یک ثبات با بازخورد خطی[۲] $(LFSR)$ با استفاده از چندجمله‌ای بازخورد[۳] $C(X) = 1 - \sum_{i=0}^{L} c_i X^i \in \mathbb{F}_q[X]$ تعریف می‌شود که L طول ثبات نامیده می‌شود. این ثبات رشته‌ی $(s_0, s_1, \cdots, s_{L-1}) \in \mathbb{F}_q^L$ را (که حالت اولیه نامیده می‌شود) با استفاده از رابطه‌ی بازگشتی زیر به یک دنباله با طول نامتناهی (که دنباله‌ی خروجی نامیده می‌شود) تبدیل می‌کند.

$$\forall t \geq 0 \text{ ، } s_{t+L} = \sum_{i=1}^{L} c_i s_{t+L-i}$$

در این صورت دنباله‌ی خروجی یک $LFSR$ بصورت $(s_t)_{t \geq 0}$ است.
در شکل زیر روند کار یک $LFSR$ به طول L را می‌بینید.



۱.۲ چندجمله‌ای بازخورد و چندجمله‌ای مشخصه

دنباله‌ی خروجی یک $LFSR$ بصورت یکتایی بوسیله ضرایب چندجمله‌ای بازخورد و حالت اولیه تعیین می‌شود. ضرایب بازخورد $c_1, c_2, \cdots, c_L$ یک $LFSR$ با طول L بوسیله‌ی چندجمله‌ای بازخورد که بصورت زیر تعریف می‌شود، مشخص می‌شوند.

$$C(X) = 1 - \sum_{i=1}^{L} c_i X^i.$$

همچنین این ضرایب را با استفاده از چندجمله‌ای مشخصه[۴] می‌توان بدست آورد:

[۲] Linear Feedback Shift Register
[۳] Feedback polynomial
[۴] Characteristic polynomial

$$C^*(X) = X^L C(\frac{۱}{X}) = X^L - \sum_{i=۱}^{L} c_i X^{L-i}.$$

مثال ۱۰ *برای یک $LFSR$ با طول ۴ در میدان $\mathbb{F}_۲$ و ضرایب بازخورد $c_۱ = c_۲ = ۰, c_۳ = c_۴ = ۱$، چندجمله‌ای بازخورد و چندجمله‌ای مشخصه به ترتیب بصورت*

$$C(X) = ۱ + X^۳ + X^۴ \in \mathbb{F}_۲[X]$$

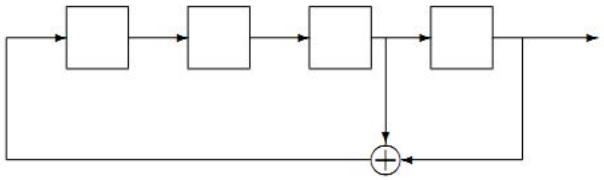
و

$$C^*(X) = ۱ + X + X^۴ \in \mathbb{F}_۲[X]$$

است.
دنباله‌ی خروجی این $LFSR$ با توجه به رابطه بازگشتی زیر تعیین می‌شود.

$$s_{t+۴} = s_t + s_{t+۱} \mod ۲$$

در شکل زیر روند تولید این دنباله را می‌بینید.



برای مثال اگر حالت اولیه را برابر $(s_۰, s_۱, s_۲, s_۳, s_۴) = (۱, ۰, ۱, ۱)$ قرار دهیم، طبق جدول زیر دنباله‌ی خروجی تولید می‌شود.

t	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
s_t	۱	۰	۱	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱
$s_{t+۱}$	۰	۱	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱	۰
$s_{t+۲}$	۱	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱	۰	۱
$s_{t+۳}$	۱	۱	۱	۰	۰	۰	۱	۰	۰	۱	۱	۰	۱	۰	۱	۱

دنباله‌ی $(s_t)_{t\geq ۰}$ متناوب نامیده می‌شود اگر عد صحیحی چون T باشد وجود داشته باشد بطوری‌که برای هر $t \geq ۰$ داشته باشیم $s_t = s_{t+T}$. کوچکترین عدد صحیحی که برای آن رابطه فوق برقرار باشد دوره‌ی تناوب دنباله نامیده می‌شود. یک دنباله‌ی متناوب با دوره‌ی تناوب T را بصورت:

$$s_۰, s_۱, \cdots, s_{T-۱}, s_۰, s_۱, \cdots = [s_۰, s_۱, \cdots, s_{T-۱}]^\infty$$

نمایش می‌دهیم.

تعریف ۱۱ *یک $LFSR$ را غیرتکین گوییم، هرگاه در چندجمله‌ای مشخصه c_L غیر صفر باشد.*

یک $LFSR$ با طول L روی $\mathbb{F}_q$ دارای q^L حالت مختلف است که حالت تمام صفر همواره به خودش انتقال می‌یابد. دنباله خروجی هر $LFSR$ غیرتکین با طول L روی $\mathbb{F}_q$ متناوب است و دوره‌ی تناوب آن حداکثر $q^L - ۱$ است، یعنی بعد از حداکثر $q^L - ۱$ بار اجرای $LFSR$ به حالت اولیه می‌رسیم.

تعریف ۱۲ *دوره‌ی تناوب چندجمله‌ای $C(X)$ برابر کوچکترین عدد صحیح و مثبت T است که $C(X) \mid (۱ - X^T)$.*

برای هر چندجمله‌ای غیرتکین $C(X) \in \mathbb{F}_q[X]$ با درجه L همواره داریم $C(X) \mid (۱ - X^{q^L - ۱})$؛ لذا $T \leq q^L - ۱$.
یک روش برای بدست آوردن دوره‌ی تناوب چندجمله‌ای $C(X)$ استفاده از روش تقسیم طولانی است. به این صورت که چندجمله‌ای ۱ را به چندجمله‌ای $C(X)$ تا زمانی که باقیمانده برابر X^N شود، تقسیم می‌کنیم (در میدان $\mathbb{F}_q$) ؛ یعنی $\frac{۱}{C(X)} = Q(X) + \frac{X^N}{C(X)}$، در این صورت دوره‌ی تناوب چندجمله‌ای $C(X)$ برابر $T = N$ است. البته الگوریتم‌های کاراتری نیز برای محاسبه دوره تناوب چندجمله‌ای‌ها وجود دارد.

تعریف ۱۳ *چندجمله‌ای $P(X) \in \mathbb{F}_q[X]$ تحویل‌ناپذیر نامیده می‌شود اگر نتوان آنرا روی $\mathbb{F}_q[X]$ به صورت حاصل‌ضرب دو چندجمله‌ای با درجه کمتر نوشت. چندجمله‌ای تحویل‌ناپذیر $P(X) \in \mathbb{F}_q[X]$ از درجه‌ی L را اولیه[۵] گوییم، هرگاه دوره‌ی تناوب آن برابر $q^L - ۱$ باشد.*

قضیه ۱ *اگر $(s_t)_{t\geq ۰}$ دنباله‌ی تولید شده بوسیله‌ی یک $LFSR$ به طول L با چندجمله‌ای بازخورد تحویل‌ناپذیر $C(X) \in \mathbb{F}_q[X]$ از یک حالت اولیه تمام ناصفر باشد، آنگاه دوره تناوب دنباله $(s_t)_{t\geq ۰}$ با دوره تناوب چندجمله‌ای $C(X)$ برابر است.*

برهان. برای اثبات این قضیه ابتدا دو لم زیر را مطرح و اثبات می‌کنیم.

لم ۲ *دنباله‌ی $(s_t)_{t\geq ۰}$ تولید شده بوسیله‌ی یک $LFSR$ به طول L روی میدان $\mathbb{F}_q$ با چندجمله‌ای بازخورد $C(X)$ است اگر و تنها اگر وجود داشته باشد چندجمله‌ای $Q(X) \in \mathbb{F}_q[X]$ با $\deg Q < L$ بطوری که*

$$\sum_{t\geq ۰} s_t X^t = \frac{Q(X)}{C(X)}.$$

علاوه بر این چندجمله‌ای Q کاملاً بوسیله‌ی ضرایب C و حالت اولیه‌ی $LFSR$ بصورت زیر مشخص می‌شود:

$$Q(X) = -\sum_{j=۰}^{L-۱} X^j \Big(\sum_{i=۰}^{j} c_i s_{j-i} \Big),$$

جائیکه $C(X) = ۱ - \sum_{i=۱}^{L} c_i X^i$.

برهان. قرار دهید

$$S(X) = s_۰ + s_۱ X + \cdots = \sum_{k=۰}^{\infty} s_k X^k.$$

و $C(X) = -\sum_{i=۰}^{L} c_i X^i$ که $c_۰ = -۱$ دراین صورت داریم:

$$S(X)C(X) = -\sum_{k=۰}^{\infty} s_k X^k \sum_{i=۰}^{L} c_i X^i = -\sum_{k=۰}^{\infty} \sum_{i=۰}^{L} s_k c_i X^{k+i}$$

اگر قرار دهیم $j \leftarrow k+i$ داریم:

$$S(X)C(X) = -\sum_{j=۰}^{\infty} \Big(\sum_{i=۰}^{\min\{j,L\}} c_i s_{j-i} \Big) X^j$$

اما برای $j \geq L$ داریم $\sum_{i=۰}^{L} c_i s_{j-i} = ۰$. بنابراین:

$$S(X)C(X) = -\sum_{j=۰}^{L-۱} \Big(\sum_{i=۰}^{j} c_i s_{j-i} \Big) X^j = Q(X)$$

جائیکه $Q(X) = q_۰ + q_۱ X + \cdots + q_{L-۱} X^{L-۱}$ و $q_j = -\sum_{i=۰}^{j} c_i s_{j-i}$.

بنابراین هر دنباله $LFSR$ تبدیل می‌شود به $S(X) = \frac{Q(X)}{C(X)}$ که $\deg(Q) < \deg(C)$.

■

[۵] Primitive

لم ۳ *اگر* $\gcd(C,Q)=1$ *و* $\deg(Q)<\deg(C)$*، آنگاه دوره تناوب چندجمله‌ای* $C(X)$ *با دوره تناوب دنباله‌ی* s *با تابع مولد* $S(X)=\frac{Q(X)}{C(X)}$ *یکسان است.*

برهان. فرض کنید دوره‌ی تناوب $C(X)$ برابر T' و دوره‌ی تناوب دنباله‌ی s برابر T باشد.
با توجه تناظرهای زیر بین توابع مولد و دنباله‌ها

$$\underbrace{[1,0,0,0,\cdots,0]}_{T\text{ positions}}^{\infty}\longrightarrow 1+X^T+X^{2T}+\cdots=\frac{1}{1-X^T}\ ,$$

$$\underbrace{[0,1,0,0,\cdots,0]}_{T\text{ positions}}^{\infty}\longrightarrow X+X^{T+1}+X^{2T+1}+\cdots=\frac{X}{1-X^T}\ ,$$

$$\underbrace{[0,0,1,0,\cdots,0]}_{T\text{ positions}}^{\infty}\longrightarrow X^2+X^{T+2}+X^{2T+2}+\cdots=\frac{X^2}{1-X^T}\ ,$$

می‌توان نتیجه گرفت که تابع مولد دنباله‌ی متناوب $s=[s_0,s_1,\cdots,s_{T-1}]^{\infty}$ تابع $S(X)=\frac{s_0+s_1X+\cdots+s_{T-1}X^{T-1}}{1-X^T}$ است. بنابراین

$$S(X)=\frac{Q(X)}{C(X)}=\frac{s_0+s_1X+\cdots+s_{T-1}X^{T-1}}{1-X^T}$$

که به این صورت می‌توان نوشت:

$$(s_0+s_1X+\cdots+s_{T-1}X^{T-1})C(X)=(1-X^T)Q(X)$$

اما $\gcd(C,Q)=1$ پس $C(X)\mid 1-X^T$ و از آنجا که T' دوره تناوب C است، پس $T'\le T$.
حال نشان می‌دهیم $T\le T'$. چون $C(X)\mid 1-X^{T'}$ پس موجود است $P(X)\in\mathbb{F}_q[X]$ که $C(X)P(X)=1-X^{T'}$. دقت کنید که چون $\deg(Q)<\deg(C)$ لذا $\deg(QP)<\deg(CP)=T'$. پس وجود دارد یک $(s'_0,s'_1,\cdots,s'_{T'-1})$ که

$$Q(X)P(X)=s'_0+s'_1X+\cdots+s'_{T'-1}X^{T'-1}\ .$$

بنابراین

$$S(X)=\frac{Q(X)}{C(X)}=\frac{Q(X)P(X)}{C(X)P(X)}=\frac{s'_0+s'_1X+\cdots+s'_{T'-1}X^{T'-1}}{1-X^{T'}}\ .$$

بنابراین

$$s=[s'_0,s'_1,\cdots,s'_{T'-1}]^{\infty}=[s_0,s_1,\cdots,s_{T-1}]^{\infty}\ .$$

که نتیجه می‌دهد $s_t=s_{t+T'}$. چون دوره‌ی تناوب دنباله s کوچکترین عدد صحیح و مثبت N است که $s_t=s_{t+N}$ برای همه مقادیر $t\ge 0$، پس $T\le T'$.

■ ■

نتیجه ۱۴ *اگر* $(s_t)_{t\ge 0}$ *دنباله‌ی تولید شده بوسیله‌ی یک* $LFSR$ *به طول* L *با چندجمله‌ای بازخورد تحویل‌ناپذیر* $C(X)\in\mathbb{F}_q[X]$ *از یک حالت اولیه تمام ناصفر باشد، آنگاه این دنباله توسط هیچ* $LFSR$*ی با طول کمتر از* L *تولید نمی‌شود.*

برهان. نتیجه‌ای که از لم اول می‌توان گرفت این است که ارتباطی یک به یک بین دنباله‌های تولید شده توسط یک $LFSR$ به طول L با چندجمله‌ای بازخورد C و کسرهای $Q(X)/C(X)$ که $\deg Q<L$ موجود است.
همچنین می‌توان نتیجه گرفت که دنباله‌ی تولید شده بوسیله‌ی یک $LFSR$ با چندجمله‌ای بازخورد C (و طول $\deg(C)$) با تابع مولد $Q(X)/C(X)$ اگر $\gcd(C,Q)\neq 1$ باشد، نیز بوسیله‌ی یک $LFSR$ با چندجمله‌ای بازخورد C' (و طول $\deg(C')<\deg(C)$) متناظر با کسر $Q'(X)/C'(X)=Q(X)/C(X)$ نیز تولید می‌شود. بنابراین همه‌ی دنباله‌های تولیدشده توسط یک $LFSR$ با چندجمله‌ای بازخورد C بوسیله‌ی $LFSR$ کوچکتری تولید می‌شوند اگر و تنها اگر C در میدان $\mathbb{F}_q$ تحویل‌ناپذیر نباشد. ■

نتیجه ۱۵ *دنباله خروجی هر $LFSR$ با طول L و چندجمله‌ای بازخورد اولیه روی $\mathbb{F}_q$ از هر حالت اولیه تمام ناصفر دارای دوره‌ی تناوب $q^L - ۱$ است. به‌علاوه، تمام حالت‌های تمام ناصفر در هر دوره دقیقاً یک‌بار ظاهر می‌شوند.*

نتیجه ۱۶ *از رابطه $S(X) = \frac{Q(X)}{C(X)}$ نتیجه می‌شود که هر دنباله‌ی تولید شده توسط یک $LFSR$ با چندجمله‌ای بازخورد C، بوسیله‌ی هر $LFSR$ی که چندجمله‌ای بازخورد آن مضربی از C باشد، نیز تولید می‌شود. این ویژگی در بعضی از حمله‌هایی که به رمزهای دنباله‌ای مبتنی بر $LFSR$ اعمال می‌شوند، مانند حمله همبستگی[۶] و حمله همبستگی سریع[۷]، مورد استفاده قرار می‌گیرد.*

[۶] correlation attack
[۷] fast correlation attack