Technische Realisierung azyklischer Zufallsfolgen, Kurzfassung,

2000, Rolf Freitag, Nürnberg, www.true-random.com

Die Realisierung von azyklischen Zufallsbitfolgen mit einer zweistufigen Autokorrelationsfunktion ist nicht trivial, da sie auf echt zufälligen Prozessen basiert und die daraus generierten Bits unabhängig sein müssen. D. h. unabhängig von allen vorhergehen oder nachfolgenden Bits muss ein Bit der Folge mit einer Wahrscheinlichkeit von 50 % ein 0-Bit oder ein 1-Bit sein; die Entropie und der Entropiebelag muss 1 Bit/Bit betragen.

Im Prinzip kann eine azyklische Zufallsbitfolge schon dadurch erzeugt werden, dass ein Signal mit der (Wiederhol-)Frequenz f_1 von einem Oszillator erzeugt wird und dieses Signal mit einer Frequenz f_2 von einem anderen Oszillator abgetastet wird. Diese Abtastwerte in digitaler serieller Form bilden eine Zufallsbitfolge, die azyklisch ist, wenn f_1 und f_2 inkommensurabel sind, es also keine natürlichen Zahlen n und m gibt, sodass $n \cdot f_1 = m \cdot f_2$ erfüllbar ist. Diese Bedingung ist gleichbedeutend damit, dass $\frac{f_1}{f_2}$ keine rationale Zahl ist und deshalb fast immer erfüllt ist, weil f_1 und f_2 im Allgemeinen irgendwelche reellen Zahlen sind (woraus folgt, dass auch $\frac{f_1}{f_2}$ irgendeine reelle Zahl ist), und weil bekanntlich fast alle reellen Zahlen irrational sind, da die Menge der rationalen Zahlen eine Lebesgue-Nullmenge ist.
Obwohl also die Wahrscheinlichkeit für $n \cdot f_1 = m \cdot f_2$ gleich null ist, zeigt sich in der Praxis aber, dass die Qualität der so erzeugten Zufallszahlen relativ schlecht ist, weil sie im Wesentlichen von dem Rauschverhalten der beiden Oszillatoren bestimmt wird, und Oszillatoren in der Regel rauscharm sind. Deshalb müssen so erzeugte Zufallszahlen nachbearbeitet werden.

Weil auch andere echt zufällige Prozesse immer mehr oder minder deutliche Korrelationen und Alterungserscheinungen zeigen, ist es daher entscheidend, solche Zufallsbitfolgen schnell und effizient in perfekt zufällige Zufallsbitfolgen zu verarbeiten. Hierfür reicht es erfahrungsgemäß aus, eine primäre nichtdeterministische Zufallsbitfolge mit einer Pseudozufallsbitfolge mittels Exklusiv-Oder (=Summe modulo 2) zu verknüpfen. Der Nachteil hierbei ist, dass die azyklische Zufallsbitfolge die Korrelationen der Pseudozufallsbitfolge teilweise enthält, und zwar umso deutlicher, je weniger Entropie oder Entropiebelag die primäre echte Zufallsbitfolge enthält. Dieses Problem kann man lösen, indem man die Modulo-2-Summe nicht mit nur einem, sondern mehreren nichtdeterministischen Zufallsbits bildet. In diesem Fall kann dann der zentrale Grenzwertsatz angewendet werden, weil das erforderliche Lindeberg-Kriterium bei der Addition von nichtdeterministischen Bits immer erfüllt ist (siehe nächste zwei Abschnitte).

1 Modulo-2-Summe von zwei Zufallsbits

Die Entropie einer Zufallsbitsequenz

$$E = -p(0) \cdot log_2(p(0)) - p(1) \cdot log_2(p(1)) \tag{1}$$

ergibt sich aus der Wahrscheinlichkeit $p(0)$ (abgek. x), dass ein Bit der Sequenz 0 ist und aus der Wahrscheinlichkeit $p(1)$ (abgek. 1-x), dass ein Bit der Sequenz 1 ist.

Damit ist es einfach, den Zuwachs an Entropie je Bit zu berechnen, den man erhält, wenn man eine Bitfolge mit einer anderen, statistisch unabhängigen mit gleichen Wahrscheinlichkeiten ($p(0)$ und $p(1)$) exklusiv verodert und so eine sekundäre Bitfolge durch bitweise Modulo-2-Addition bildet:

$$\begin{aligned} E_1 - E_2 = -(x^2 + (1-x)^2) \cdot log_2(x^2 + (1-x)^2) \quad & -2 \cdot x \cdot (1-x) \cdot log_2(2 \cdot x \cdot (1-x)) \\ +x \cdot log_2(x) + (1-x) \cdot log_2(1-x) & \end{aligned} \tag{2}$$

mit den Abkürzungen $x = p(0)$ und $1 - x = p(1)$.

Für nicht perfekt zufällige primäre echte Zufallsbitsequenzen, also $0 < x < 1, \quad x \neq 0.5$, ist dieser Zuwachs positiv und größer null, wie sich auch beim Auftragen des Zuwachses $y = E_1 - E_2$ über $x = p(0)$ zeigt: (Abb. 1)

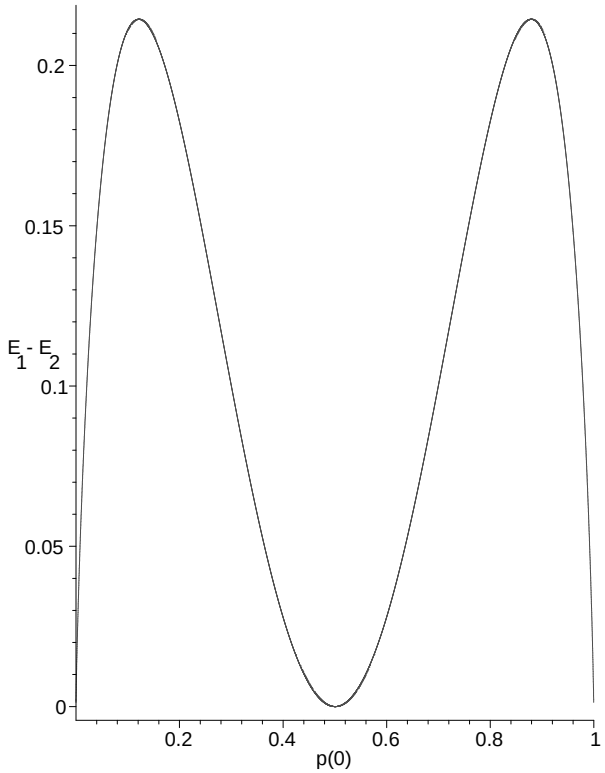

Abb. 1: Entropiezuwachs durch Exklusiv-Oder-Verknüpfung von zwei Zufallsbits, aufgetragen über p(0) (abgek. x).

Durch rekursive Anwendung ergibt sich hieraus, dass die Modulo-2-Addition von 2^n ($n > 0$) statistisch unabhängigen Bitsequenzen mit gleichen Wahrscheinlichkeiten eine entropiereichere sekundäre Bitsequenz ergibt, die umso entropiereicher (=zufälliger) ist, je größer n ist.

Weil die Gleichung 2 unabhängig von den einzelnen Bits gilt, werden durch die Modulo-2-Addition auch die Korrelationen innerhalb der sekundären Bitsequenz abgeschwächt, sodass auch die Markow-Entropien und der Entropiebelag erhöht werden.

Wie sich numerisch leicht zeigen lässt, ist das Voraussetzen von statistisch unabhängigen Bitsequenzen mit gleichen Wahrscheinlichkeiten in der Regel nicht nötig. Dadurch ist es in der Praxis fast immer möglich, mittels Modulo-2-Addition von 2^n primären Zufallsbitfolgen eine Zufallsbitfolge mit erhöhter Entropie zu erzeugen.

2 Modulo-2-Summe von n Zufallsbits und der zentrale Grenzwertsatz

Nach dem Zentralen Grenzwertsatz ist die Wahrscheinlichkeitsdichte der Summe s von $n \gg 1$ echt zufälligen Bits die Normalverteilung, weil eine Summe von Bits automatisch die Lindebergsche Bedingung erfüllt. Der zentrale Grenzwertsatz gilt zwar genau genommen nur für unendliches n, aber er ist meist schon bei ungefähr 10 in guter Näherung gültig.

Liegt das Maximum der Normalverteilung p_v bei exakt $m + 0,5$ ($m \in \mathbb{N}$), dann ist die Amplitude der Normalverteilung bei $m + 0,5 - k/2$ dieselbe wie bei $m + 0,5 + k/2$. Weil die Modulo-2-Summe bei $m + 0,5 - k/2$ und $m + 0,5 + k/2$ einmal 1 und einmal 0 ist, bedeutet dies, dass sich für jeden k-Wert, und damit auch für die gesamte Summe, eine 50 % Wahrscheinlichkeit für eine 0 und eine 1 ergibt. Dies ist der "best case", denn es bedeutet, dass die Sekundärbits eine Entropie von 1,0 Bit/Bit besitzen.

Im "worst case" liegt das Maximum der Normalverteilung p_v bei m ($m \in \mathbb{N}$), und der Betrag der Differenz der Wahrscheinlichkeit, dass die Modulo-2-Summe null ist minus der Wahrscheinlichkeit, dass die Modulo-2-Summe eins ist, ergibt sich zu:

$$\mid p(0) - p(1) \mid_{worst\ case} = \frac{1}{\sigma \cdot \sqrt{2 \cdot \pi}} \cdot 2 \cdot \sum_{k=1}^{\infty} \left(e^{-\frac{(2 \cdot k - 1)^2}{2 \cdot \sigma^2}} - e^{-\frac{(2 \cdot k)^2}{2 \cdot \sigma^2}} \right) \quad . \qquad (3)$$

Die Standardabweichung σ ist proportional zu $\sqrt{n}$ ("ars conjectandi"), sodass $\sigma = c \cdot \sqrt{n}$ mit der Konstanten c eingesetzt werden kann:

$$\mid p(0) - p(1) \mid_{worst\ case} = \frac{\sqrt{2}}{c \cdot \sqrt{n \cdot \pi}} \cdot \sum_{k=1}^{\infty} \left(e^{-\frac{(2 \cdot k - 1)^2}{2 \cdot c^2 \cdot n}} - e^{-\frac{(2 \cdot k)^2}{2 \cdot c^2 \cdot n}} \right) \quad . \qquad (4)$$

Dieser Ausdruck sinkt streng monoton mit steigendem n und der Grenzwert für $n \to \infty$ ist null (Abb. 2).

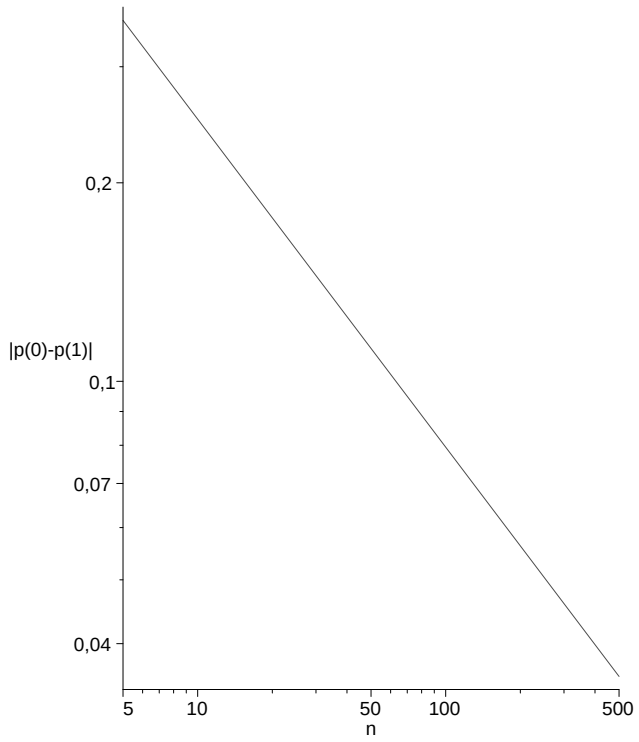

Abb. 2: Entropiezuwachs durch Exklusiv-Oder-Verknüpfung von n Zufallsbits im “worst case” , aufgetragen über n.

Somit ergibt sich also auch im “worst case” aus mehreren primären echt zufälligen Bits mit wenig Entropie mittels Modulo-2-Addition ein sekundäres echt zufälliges Bit mit mehr Entropie.
Weil die Gleichung 4 unabhängig von den einzelnen Bits gilt, werden durch die Modulo-2-Addition auch die Korrelationen innerhalb der sekundären Bitsequenz abgeschwächt, sodass auch die Markowentropien erhöht werden.

Der Vorteil hierbei ist, dass die primären Bits nicht statistisch unabhängig sein müssen und zudem die Summe auch Pseudozufallsbits enthalten kann, wenn ausreichend viele echte Zufallsbits in der Summe enthalten sind. Dadurch können mit Pseudozufallsbitgeneratoren gezielt statistische Auffälligkeiten der echt zufälligen Bits beseitigt werden.
Dies ermöglicht die Erzeugung von praktisch perfekt zufälligen Zufallsbitfolgen mit einem relativ kleinen Aufwand, denn die Erzeugung von relativ guten Pseudozufallsbitfolgen ist mit PN-Generatoren mit wenig Aufwand leicht zu realisieren und die primären echten Zufallsbitfolgen können z. B. mit Ringoszillatoren der mittleren Frequenz f_1 auf einem digitalen IC erzeugt und mit der Taktfrequenz f_2 verarbeitet werden.
Deshalb wurde hierzu das Patent 19926640 (Verfahren zur Erzeugung von echten Zufallszahlen sowie Zufallszahlengenerator) Anfang 2002 erteilt.