Generación y Caracterización de Secuencias PRN

Autor: Hernández González, Abel

Director/es: Gómez Pérez, Paula

Contacto: Escuela Naval Militar. Centro Universitario de la Defensa/paula@cud.uvigo.es

---

Resumen:

En este trabajo se ha llevado a cabo un estudio riguroso y exhaustivo de las secuencias PRN (Pseudo-Random Noise), que pretende ofrecer una base para el diseño o el análisis de sistemas de tecomunicación o, incluso, de información.

Las secuencias PRN (Pseudo-Random Noise) tienen características asimilables al ruido, cualidad ésta que las hace muy atractivas para determinadas aplicaciones civiles y militares.

Dada la variedad de estas secuencias, se ha pretendido cubrir con el estudio un ambicioso rango de secuencias PRN, incluyendo los principales tipos: caóticas, de longitud máxima, de Kasami y Gold.

Entre las conclusiones más destacadas que se alcanzan, hay que mencionar que todas ellas logran un gran reparto en banda de la potencia, muy deseable en sistemas de espectro ensanchado, que las proporciona propiedades inmunidad frente al ruido y la interferencia.

Salvando lo anterior, se concluye que, de las secuencias analizadas, las que presentan una mejor autocorrelación son las caóticas y las secuencias PN (Pseudo-Noise) de longitud máxima, dado que las de Kasami y las Gold presentan un rizado de la función para desplazamientos mayores de un chip.

Desafortunadamente, las secuencias PN de longitud máxima presentan, salvo grupos muy reducidos, una mala correlación cruzada, que las descarta para aplicaciones de acceso compartido al medio. Por su parte, las secuencias de Kasami y de Gold consiguen proporcionar grandes familias de secuencias con buenas propiedades de correlación cruzada.

Palabras clave: secuencia, chip, autocorrelación, correlación, potencia, pseudoaleatorio.

---

1. Introducción

Este trabajo pretende ser un estudio riguroso y exhaustivo de las secuencias PRN (Pseudo-Random Noise) que pueda servir de base para el diseño o el análisis de sistemas de tecomunicación o, incluso, de sistemas de información.

Por consiguiente, el trabajo presenta dos vertientes diferenciadas, aunque interrelacionadas: la generación de las secuencias y la caracterización de las mismas.

A su vez, se ha pretendido ofrecer una amplia panorámica, extendiendo los análisis a los principales tipos de secuencias PRN: caóticas, de longitud máxima, de Kasami y Gold.

Estos códigos han sido empleados tradicionalmente en sistemas de telecomunicación de espectro ensanchado de uso militar, dada su robustez frente al ruido y las interferencias. Las propiedades de baja correlación cruzada de algunos tipos de secuencias ha impulsado su extensión al ámbito civil, generalizándose su uso en sistemas de acceso múltiple al medio (además de en GPS, entre otros).

Las secuencias pseudoaleatorias serán, generalmente, señales digitales binarias +/-V, es decir, polares. En el marco de las comunicaciones de espectro ensanchado, para diferenciar la secuencia pseudoaleatoria de la señal de información, los bits de la secuencia pseudoaleatoria se designan como chips.

La criptografía, la ciberseguridad y las tecnologías de la información, en general, constituyen hoy día ámbitos de aplicación de las mismas poco explorados, con mucho potencial, donde las capacidades de cómputo actuales y la ingeniería de servicios pueden despertar el interés por ellas en cualquier momento.

2. Desarrollo

En la vertiente más teórica se explica el proceso de generación de los cuatro tipos de secuencias PRN consideradas: caóticas, de longitud máxima, de Kasami y Gold. Se incluyen diversos desarrollos matemáticos para explicar algunas de las propiedades.

En la vertiente experimental se efectúan una infinidad de simulaciones en Matlab. En el capítulo 4 y en los Apéndices se incluye un extracto de las simulaciones y análisis realizados.

Del análisis de las gráficas (visual y cuantitativo) y del de las distintas tablas confeccionadas se alcanzan las conclusiones relacionadas a continuación, que incluyen también consideraciones relativas a la simulación.

3. Conclusiones

Conclusiones generales de las secuencias PRN.

- En ausencia de ruido, a los efectos de obtener gráficamente la función de autocorrelación de señales digitales o la correlación cruzada de una pareja de ellas, éstas pueden ser muestreadas empleando una única muestra por chip.
- Si se desea obtener el valor de las propiedades de correlación para desplazamientos distintos de los múltiplos enteros de un periodo de chip, será necesario tomar varias muestras de la secuencia por cada chip.
- La autocorrelación de secuencias digitales es una función simétrica, es decir: $\mathcal{R}_c[\tau] = \mathcal{R}_c[-\tau]$.

- El máximo de la función autocorrelación coincide con la potencia media de la señal.
- Presentan muy baja autocorrelación para cualquier desplazamiento τ que diste más de un chip del máximo de la función (y de sus infinitas réplicas, en el caso de ser periódica).
- La función de correlación cruzada de una pareja de secuencias, tomadas en un determinado orden, muestra simetría especular respecto de la función resultante en el caso de que las secuencias se tomasen en orden inverso: $\mathcal{R}_{c_1c_2}[\tau] = \mathcal{R}_{c_2c_1}[-\tau]$.
- Las secuencias PRN logran un buen reparto en banda de la potencia de señal, propiedad necesaria en aplicaciones de espectro ensanchado.
- Tienen un espectro de tipo 'sinc cuadrado', estando concentrada la mayor parte de la potencia en el lóbulo principal, es decir, en frecuencias inferiores al régimen de chip.

Conclusiones específicas de las secuencias caóticas.

- Las secuencias generadas por un sistema caótico a partir de dos estados iniciales cuyo valor difiera muy poco tienden a ser incorreladas al poco tiempo.
- La función de autocorrelación de secuencias caóticas indefinidas tiende a ser plana, de valor nulo, para desplazamientos mayores de un chip.
- La función de correlación cruzada de secuencias caóticas indefinidas tiende a cero para cualquier desplazamiento τ. En todo caso, la amplitud de la correlación parcial queda acotada en un rango más pequeño a medida que aumenta la longitud de la pareja de subsecuencias correladas.
- Trabajando con secuencias de longitud finita aparecen picos secundarios en la autocorrelación parcial. Por tanto, su aplicación a sistemas de acceso múltiple al medio requerirá el empleo de códigos lo suficientemente largos.
- El promedio de un determinado número de autocorrelaciones parciales, a partir de la extracción de subsecuencias no solapadas en el tiempo, constituye una mejor aproximación a la autocorrelación de la secuencia caótica indefinida que la del promedio de una sucesión de subsecuencias desplazadas chip a chip.
- El mecanismo de promediado de subsecuencias consecutivas no solapadas constituye, en definitiva, una muy buena aproximación a la autocorrelación de la secuencia caótica indefinida, permitiendo aproximarla con un número relativamente reducido de chips.
- Los picos secundarios de la autocorrelación parcial se cancelan o compensan en la gráfica de la autocorrelación promedio. Esta afirmación lleva implícita que no se tomen subsecuencias solapadas a la hora de calcular la aproximación a la autocorrelación de la secuencia caótica indefinida.
- Por lo general, al aumentar la longitud de las subsecuencias caóticas mejoran sus propiedades de correlación cruzada. Esta consideración habrá que tenerla en cuenta a la hora de establecer el tamaño de los códigos empleados en entornos de acceso multiple al medio.

Conclusiones específicas de las secuencias PN de longitud máxima.

- Son secuencias periódicas, cuyo periodo tiene una longitud de $2^N - 1$ chips, donde N es el número de registros del generador linealmente realimentado.
- Cada ciclo tiene $2^N / 2$ 'unos'.

- La autocorrelación de una secuencia PN indefinida es una función periódica de periodo *L* chips, al igual que el de la secuencia. Por tanto, los máximos de la función se encuentran posicionados en los desplazamientos múltiplos enteros del periodo.
- La función de autocorrelación de la secuencia indefinida muestra un pedestal o suelo de autocorrelación, que tiende a cero a medida que aumenta la longitud del periodo de la secuencia.
- Para obtener, mediante simulación, una buena aproximación de las funciones de autocorrelación o de correlación cruzada de secuencias indefinidas, no resulta suficiente con considerar un único periodo de las secuencias, sino que ha de ser un número suficientemente grande de ciclos, debiéndose acotar la observación a la región central de las funciones.
- El suelo de la autocorrelación parcial se suaviza al aumentar el número de periodos de la ventana de correlación de las simulaciones.
- La correlación cruzada de secuencias PN indefinidas es una función periódica de periodo *L* chips.
- Por lo general, no presentan buenas propiedades de correlación cruzada, salvo determinadas parejas de secuencias, denominadas preferentes, cuya función de correlación presenta únicamente tres valores característicos.
- La separación entre componentes espectrales es R_{chip}/L, de tal modo que en cada lóbulo hay *L-1* componentes, siendo *L* el periodo de la secuencia expresado en chips.
- La envolvente de potencia espectral disminuye conforme aumenta la longitud del periodo de la secuencia, al quedar repartida la misma potencia de señal entre un mayor número de componentes.

Conclusiones específicas de las secuencias de Kasami.

- Una familia de secuencias de Kasami proporciona un conjunto de secuencias con buenas propiedades de correlacion cruzada, mayor que los conjuntos preferentes que pueden obtenerse de secuencias PN de longitud máxima, para una misma longitud de periodo.
- El número de secuencias de Kasami que integran una familia varía dependiendo de la secuencia PN de longitud máxima que se tome de base.
- Todas las secuencias de una familia de Kasami son periódicas, de igual longitud de periodo que la secuencia PN de longitud máxima en que se basen.
- Su función de autocorrelación presenta un rizado para desplazamientos mayores de un chip respecto de los máximos absolutos de la función.
- El rizado de la autocorrelación queda determinado por tres valores característicos, tendiendo a ser simétrico a medida que aumenta la longitud de la secuencia.
- El rizado de la autocorrelación disminuye a medida que aumenta la longitud del periodo de la secuencia.
- La función de correlación cruzada de secuencias de la misma familia presenta el mismo rizado que la función de autocorrelación de las secuencias.
- Las parejas de secuencias de una misma familia presentan mejores propiedades de correlación cruzada que las parejas preferentes de secuencias PN, tendiendo a ser el rizado en el primer caso la mitad que en el segundo, a medida que aumenta la longitud del periodo.

Conclusiones específicas de las secuencias Gold.

- El número de secuencias Gold que integra una familia es muy grande, siendo: $M = 2^N + 1$. Este número resulta muy superior al número de secuencias que integra una familia de Kasami.
- Todas las secuencias de una familia Gold son periódicas, de periodo de $2^N - 1$ chips, al igual que el de las secuencias preferentes en que se basan.
- No todas las secuencias Gold tienen $2^N / 2$ unos, existiendo en cada familia tres posibilidades distintas en cuanto al número de unos.
- Su función de autocorrelación presenta un rizado para desplazamientos mayores de un chip respecto de los máximos absolutos de la función.
- El rizado de la autocorrelación queda determinado por tres valores característicos, tendiendo a ser simétrico a medida que aumenta la longitud de la secuencia. No obstante, para longitudes de periodo bajas se encuentran algunas secuencias para las que desaparece el valor extremo inferior.
- El rizado de la autocorrelación disminuye a medida que aumenta la longitud del periodo de la secuencia.
- El rizado de la autocorrelación coincide con el de las parejas preferentes de secuencias PN de la misma longitud de periodo.
- La función de correlación cruzada de secuencias de la misma familia presenta el mismo rizado que la función de autocorrelación las secuencias.
- No todas las parejas de la familia muestran los tres valores característios de correlación, encontrándose algunas parejas en las que desaparece la cota extrema inferior, para longitudes de periodo bajas.
- Las secuencias GPS que identifican los satélites de la red tienen un periodo de 1023 chips, de los cuales 512 son unos.
- El rizado de las funciones de autocorrelación y correlación cruzada de las secuencias GPS presentan ambas cotas extremas características, positiva y negativa.

Agradecimientos

A los miembros de mi familia, sin cuya comprensión, paciencia y ánimo no habría podido culminar este estudio. Soy consciente de las muchas facilidades que me han prestado, disculpándome siempre del tiempo de dedicación del que les he privado.

A mi directora de TFM, por los ánimos y colaboración que me ha brindado en todo momento.

Referencias

Savo Glisic y Branka Vucetic, *Spread Spectrum CDMA Systems for Wireless Communications.* Artech House, 1997.

José M. Hernando, *Comunicaciones Móviles.* Centro de Estudios Ramón Areces, 1997.

Robert B. Ward, "*Acquisition of Pseudonoise Signals by Sequential Estimation*", IEEE Transactions on Communication Technology, vol. COM-13, pp.475-483, Diciembre 1965.

Andreas Polydoros y Charles L. Weber, "*A Unified Approach to Serial Search Spread-Spectrum Code Acquisitión-Part II: A Matched-Filter Receiver*", IEEE Transactions on Communications, vol. COM-32, Nº5, pp.550-551, Mayo 1984.

J.-F. Beaumont, "*RTL Design of a Generic Pseudonoise Generator*", Defence R&D 2004-176, Ottawa (Canadá), Septiembre de 2004.

M. Gulotta, "*HDL Coding for Pseudo-Random Noise Generators*", Xcell Journal, Nº35, pp. 43-45, verano 2002.

New Wave Instruments, "*LRS-200 Family Spread Spectrum Generators*", Septiembre de 2001. (http://www.newwaveinstruments.com/literature/documents/pdf/LRS-200_brochure.pdf).

S. Azou, G. Burel y C. Pistre, "A Chaotic Direct-Sequence Spread-Spectrum System for Underwater Communication", *IEEE-Oceans'2002*, vol. 4, pp.2409-2415, Octubre 2002.

G. Heidari-Bateni y C. D. McGillem, "A Chaotic Direct-Sequence Spread Spectrum Communication System", *IEEE Transactions on Communications*, vol. 42, Nº2, pp.1524-1527, 1994.

https://es.wikipedia.org/wiki/GPS#Evolución_del_sistema_GPS.

M. Carmen Pérez Rubio, "*Generación y Correlación Eficiente de Códigos Binarios Derivados de Conjuntos de Secuencias Complementarias para Sistemas Ultrasónicos*", Escuela Politécnica Superior de la Universidad de Alcalá, 2009.