The ~~Da Vinci~~ Galileo Code and Others

GUENTER W. HEIN, JOSE-ANGEL AVILA-RODRIGUEZ, STEFAN WALLNER

GNSS signals might fairly be characterized as an enigma wrapped inside a conundrum. More than any others, two factors give the signals this quality: spread spectrum techniques and their code structure. The first hides the signals in a "cellar" below the thermal noise floor of the RF spectrum; the second disperses them into a long and apparently random sequence of digits. The advent of Europe's Galileo system and introduction of new GPS signals stimulated a re-examination of the subject of codes, buttressed by advances in electronics that allowed new approaches to implementing codes in a GNSS receiver. This column explores the growing categories of codes, their production, and the qualities that make them suitable for use in GNSS systems. Along the way, we take a brief excursion to discover the surprising genesis of spread spectrum radio in the collaboration of a glamorous actress and an avant-garde pianist.

Codes are a fundamental element in any code division multiple access (CDMA) system such as GPS and Galileo, because these codes are the tool that enables a GNSS receiver to distinguish one satellite from another. In spite of their great importance, no great innovations have been made in the world of satellite navigation in this area — not since GPS used the Gold codes for the first time in its L1 C/A signal introduced nearly 30 years ago.

With GIOVE-A, however, the first Galileo test satellite is now in space. And, together with new signals and new technologies, new code concepts developed in recent years will appear in Galileo transmissions. Galileo will broadcast for the first time so-called random codes, which are codes optimized in a highly multidimensional space to make them look as random as possible.

But Galileo is not alone in bringing new concepts into the world of GNSS. Modernized GPS signals also use new structures of codes based on so-called Legendre sequences, which will be applied for the very first time in navigation.

Given the great importance that codes play in any GNSS system that relies on CDMA and more generally, on spread spectrum (SS) communications, SS techniques will be an important focus of this paper. This column, therefore, will begin by discussing various techniques that rely on codes and the history behind them. Then we will concentrate on the many possibilities that exist to generate pseudorandom codes, giving special attention to those code structures that GPS and Galileo will be implementing in the near future.

Spread Spectrum Communications

Spread spectrum radio communications stem from the work of Hollywood actress Hedy Lamarr and the pianist George Antheil who described in 1941 a secure radio link to control torpedos and received for that U.S. patent number 2,292,387. (See the sidebar, "Player Pianos, Sex Appeal, and Patent No. 2, 292, 387" that begins on page 64.) Although the idea was not taken seriously at the beginning and was even forgotten, the scientific community rediscovered it in

1957 at the Sylvania Electronic Systems Division.

Today, spread spectrum radio has become one of the most important modulation techniques, covering completely different applications ranging from 3G mobile telecommunications, W-LAN, and Bluetooth to satellite positioning systems such as GPS and Galileo.

In spread spectrum communications a higher-frequency signal is injected into a baseband signal bandwidth. This results in the energy used in transmitting the information of the baseband signal being spread over a wider bandwidth as shown in Figure 1. Typically, the SS power level drops below the RF noise floor, which makes the SS signal invisible for unauthorized users. The ratio (in decibels) between the spread baseband and the original signal is called processing gain (see Figure 1). Typical SS processing gains run from 10dB to 60dB.

The importance of spread spectrum can be seen if we take a look at the well-known Shannon and Hartley channel-capacity theorem:

$$C = B\log_2\left(1+\frac{S}{N}\right)$$

where

- C is the channel capacity in bits per second (bps). This is the maximum data rate for a theoretical bit-error rate (BER) and represents the amount of information allowed by the communication channel.
- B is the required channel bandwidth in Hertz,
- and S/N is the signal-to-noise power ratio and describes the environmental conditions or the physical characteristics of the channel.

An elegant interpretation of this equation, especially valid for difficult environments with low S/N ratios, is that one can maintain or even increase the communication performance (high channel capacity C) by allowing or injecting more bandwidth (high B), whatever the level of the signal is.

After some math, if we slightly modify the previous equation and assume that the S/N is usually low, as it is the case in GNSS applications, Shannon's expression simplifies to

$\frac{C}{B} \approx 1.433\frac{S}{N}$ or roughly,

$\frac{C}{B} \approx \frac{S}{N}$ which can also be expressed as

$\frac{N}{S} \approx \frac{B}{C}$. This last expression says that to send an error-free information for a given noise-to-signal ratio in a channel, we only need to perform the fundamental SS signal-spreading operation: increase the transmitted bandwidth.

Not So Simple

The SS principle seems simple and evident, but its implementation is complex. In order to accomplish this objective, different SS techniques are available, but they all have one thing in common: they perform the spreading and despreading operation by means of a pseudo random noise (PRN) code attached to the communication channel. The manner of inserting this code into the transmitting chain before the antenna is actually what defines the particular SS technique in question, as Figure 2 shows in detail.

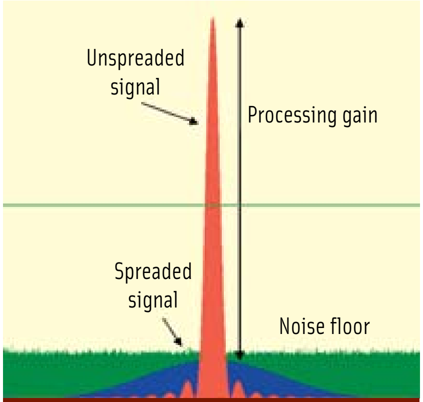


FIGURE 1 Spread Spectrum despreading operation. The desired signal (blue) is below the noise floor (green) but after correlation in the receiver, it unspreads (red) over the noise floor making detection possible. The ratio between the unspread signal and the spread signal is the processing gain.

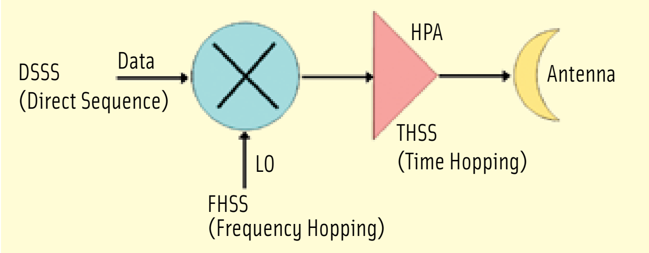


FIGURE 2 SS techniques classification depending on the point in the system at which the PRN code is inserted in the communication channel

According to this, we distinguish between:

- *Direct Sequence Spread Spectrum* (DSSS) when the PRN is inserted at the data level. In practice, the pseudo-random sequence is mixed or multiplied with the information signal. This is the way GPS and Galileo work.
- *Frequency Hopping Spread Spectrum* (FHSS) when the PRN acts at the carrier-frequency level. Applied at the LO stage, FHSS PRN codes force the carrier-frequency to change or hop according to the pseudo-random sequence. The bandwidth of the modulated signal remains unchanged when compared to the original signal and, although the desired signal power is above the noise level, it is secured because an unauthorized user never knows where the signal will be placed in the frequency domain after the next hop and how long it will stay at the new center frequency. The Bluetooth technology makes use of FHSS.
- *Time Hopping Spread Spectrum* when the PRN acts as a switch to the transmitted signal.

It is, of course, possible to mix all the above techniques to form a hybrid SS technique, such as DSSS + FHSS. DSSS and FHSS are the two techniques most in use today.

The spreading operation, as the name clearly says, consists of spreading the desired signal below the noise floor. In contrast, during the despreading operation, when the received signal is correlated with the correct code the desired signal will "unspread," rising over the noise floor while unwanted signals will remain below it.

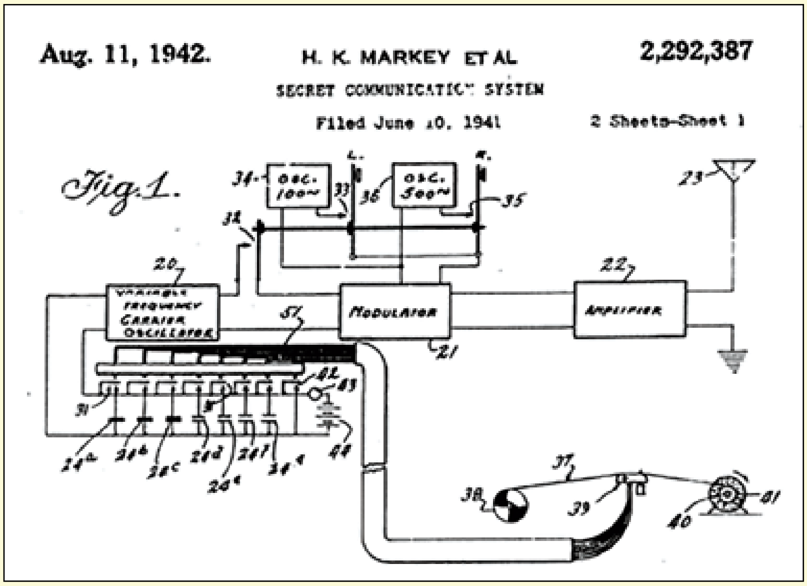
One might think that spreading a signal across a wide bandwidth does not spare the limited frequency resource we

Working Papers *continued on pg 66.*

Player Pianos, Sex Appeal, and Patent No. 2,292,387

ELIZA SCHMIDKUNZ

John Kobal Foundation/Getty Images



Hedwig Kiesler Markey AKA Hedy Lamarr in a 1944 movie publicity shot from "The Conspirators." At right, the patent drawings for the "Secret Communications System" she proposed with composer George Antheil.

Here's the concept: A supremely gorgeous Hollywood star and a Paris expatriate composer develop a secret new technology to thwart Nazi torpedoes during World War II . . . the same year that "Casablanca" is released on the big screen.

It is simply too good to be true.

But by now we know that Hedy Lamarr and George Antheil were awarded U.S. Patent No. 2,292,387 on August 11, 1942 for a "Secret Communication System." And that, indeed, the two artists invented the "frequency hopping" method of radio signal transmission, later to be known as "spread spectrum." As they explained in their patent application:

> This invention relates broadly to secret communication systems involving the lie of carrier waves of different frequencies and is especially useful in the remote control of dirigible craft, such as torpedoes. . .
>
> Briefly, our system as adapted for radio control of a remote craft employs a pair of synchronous records, one at the transmitting station and one at the receiving station, which change the tuning of the transmitting and receiving apparatus from time to time,...we contemplate employing records of the type used for many years in player pianos, and which consist of long rolls of paper having perforations variously positioned in a plurality of longitudinal rows along the records. In a conventional Player Piano record there may be 88 rows of perforations. And in our system such a record would permit the use of 88 different carrier frequencies, from one to another of which both the transmitting and receiving station would be changed at intervals. . .

How did it happen?

Hedy Lamarr, born Hedwig Kiesler in 1913 or 1914 to a Vienna banking family, did not study electrical engineering. She studied at Max Reinhardt's famous Berlin acting school and was the first actress to appear (tastefully) nude in a major motion picture, *Ekstase*, in 1933. Hitler's Germany banned the film because Kiesler was Jewish. The United States banned the film because it was erotic.

That same year, the young actress married a husband 14 years her senior. Austrian "Cartridge King" Fritz Mandl was director general of weapons manufacturer Hirtenberger Patronenfabrik. The year of his marriage, Mandl was embroiled in a notorious illegal arms transport scandal, the "Hirtenberger Waffenaffaire," in which his company smuggled German and Austrian weapons out of the country under Swiss labels.

The company made shells and grenades as well as aircraft from the mid-1930s on and supplied arms for Mussolini's 1935 invasion of Africa. Mandl was also interested in control systems. He frequently entertained key buyers and sellers of arms — as well as Hitler and Mussolini themselves — during the run-up to World War II. The bright Madame Mandl's role as hostess provided her link to discussions of weapons technology and, most likely, radio-controlled torpedoes and the need for an anti-jamming device.

The Esatet of George Anthiel

American composer and pianist George Antheil in New York, 1927

Within four years of her unhappy marriage, Madame Mandl had escaped her domineering husband and sailed to the United States, where she eventually became citizen in 1953. She continued her acting career for film factory Metro Goldwyn Mayer, whose legendary boss, Louis B. Mayer, renamed her "Lamarr." His publicity department marketed her as "the most beautiful girl in the world."

Meanwhile, George Antheil had been composing movie scores in Hollywood since his return from Europe in 1933.

Antheil was born in Trenton, New Jersey in 1900. In the 1920s, he joined the Lost Generation in Paris, where he lived above Sylvia Beach's famous Left Bank bookstore, Shakespeare & Company. He made a name for himself as a daring composer and concert pianist in Paris and Berlin. He said of his most famous piece - Ballet Mecanique " [it is] the first piece of music that has been composed OUT OF and FOR machines, ON EARTH."

The *Paris Tribune* announced the first performance in 1924, saying, "Paris will hear the strident screech and crash of giant machines evocative of modern industrial America very shortly . . . "Ballet Mechanique.". . . will be played on four player pianos simultaneously, with electricity as the motive power and a further volume of sound supplied by four electric bells, and two electric motors driving a steel propeller and a wooden rattle. . .

In 1940, the renamed Hedy Lamarr met Antheil at a Hollywood party. The two made a perfect pair — technologically if not romantically.

Lamarr had an idea for an anti-jamming device for radio controlled torpedoes. Antheil's artistic use of machines foreshadowed the electronic age. A 1990 *Forbes* magazine article on the pair said, "Antheil understood instantly that synchronizing a series of split-second hops between radio frequencies would be no more difficult — than synchronizing player pianos."

Lamarr talked about quitting MGM and working for the National Inventor's Council (NIC), a government agency formed during WWII as a technology transfer link between citizen inventors and the military. She submitted her concept, and the NIC encouraged Lamarr and Antheil to develop it into a patentable idea.

Hedy Lamarr filed the patent as Hedwig Kiesler Markey, her name in private life during her marriage to screenwriter Gene Markey. For years, no one made the connection between the patent holder and the movie star.

The War Office immediately classified it, and the patent lapsed 17 years later. Lamarr and Antheil apparently considered it their contribution to the war effort and neither made money from their brilliant idea until 1998, when wireless technology developer Wi-LAN, Inc. acquired a 49 percent claim to the patent from Lamarr for an undisclosed amount of stock.

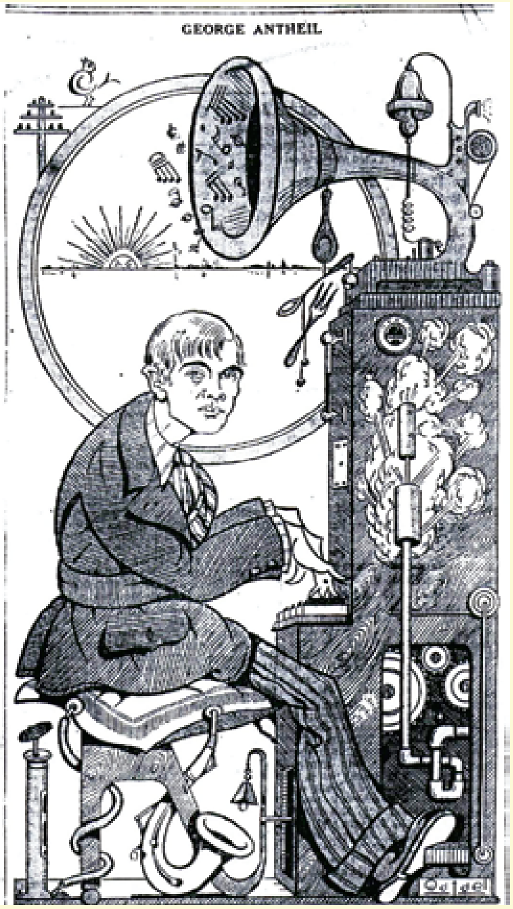
Antheil continued to compose a number of Hollywood movie scores, among them *The Plainsman* (1936) and *In a Lonely Place* (1950). He died in 1959.

Lamarr made many films, most notably *Samson and Delilah* (1949). In 1997, three years before her death, she was honored by the Electronic Frontier Foundation for her contributions to wireless technology. The EEF is a civil liberties advocacy organization that investigates, among other things, patent abuses.

Today, No. 2,292,387 is considered the foundational patent for spread spectrum technologies.

And the story behind it is every bit as good as "Casablanca." IG

Eliza Schmidkunz is director of marketing for Inside GNSS and a graduate of the University of Oregon School of Journalism.



Working Papers *continued from pg 63.*

wanted to use more efficiently with this technique. But, in fact, that use of a wide slice of radio spectrum is well compensated for by the possibility of many users to share the enlarged frequency band, which can employ different PRN codes optimized to be almost orthogonal with each other. Thus, many signals can operate in the same swath of spectrum with receivers able to distinguish the desired signals from the others.

Now that we have gained some insight in the SS techniques, let's summarize the main characteristics of spread spectrum communications:

- Wideband technology
- Resistance to interference and enhanced antijamming capability. Intentional or unintentional interference and jamming signals are rejected.
- Resistance to interception. Only if we apply the right code to the right signal (satellite) can we decode it. Indeed, without the right code, the SS signal appears as noise or as an interferer. Even better, signal levels can be below the noise floor, because the spreading operation reduces the spectral density. The message is thus made invisible, an effect that is particularly strong with the DSSS technique. Other receivers cannot "see" the transmission and only register a slight increase in the overall noise level.
- Resistance to fading (multipath effects). This is of great importance, especially for GNSS, because wireless channels often include multiple-path propagation. As it is well known, multipath is one of the most important sources of error in satellite navigation.

Pseudorandom noise (PRN) seems on observation to lack a definite cyclical pattern but, in fact, does follow a deterministic pattern that repeats itself eventually.

It is important to note that SS is not a modulation scheme, and thus it must not be confused with other types of modulation. One can, for example, use SS techniques to transmit a signal modulated by means of frequency shift keying or binary phase-shift keying. So far, three main signal transmission methods are available:

- *FDMA or Frequency Division Multiple Access.* FDMA allocates a specific carrier frequency to a communication channel, and the number of different users is limited to the number of slices in the frequency spectrum. FDMA is the least efficient in term of frequency-band usage. Glonass is the only satellite navigation system using FDMA.
- *TDMA: Time Division Multiple Access.* With TDMA different users speak and listen to each other according to a defined allocation of time slots. Thus, different communication channels can be established for a unique carrier frequency. Examples of TDMA systems are GSM, DECT, TETRA, and IS-136.
- *CDMA: Code Division Multiple Access.* CDMA access relies on a specific code. In that sense, spread spectrum is a CDMA access. The code must be defined and known in advance at the transmitter and receiver ends. This has important implications in the code design as we will see later. GPS and Galileo are two very significant examples of CDMA in which every satellite is assigned a different code. This enables the receiver to determine the satellite from which each signal is coming and, consequently, to help the receiver calculate its position by simultaneous ranging to multiple satellites.

Not So Random Noise

Codes are digital sequences that, in order to achieve the benefits that we have described, must be as long and as random as possible. That is equivalent to saying they must appear as "noise-like" as possible. This is of major importance because the robustness of the spreading and despreading operations depends on the quality of the code.

Of course, perfectly random codes would be optimal. In such an ideal case, we could have an infinite number of users with each completely distinguishable from one another. But equally important is that the codes must remain reproducible. Otherwise, the receiver will be unable to extract the message that has been sent. This is the reason why the sequence is said to be "nearly random" or pseudo-random.

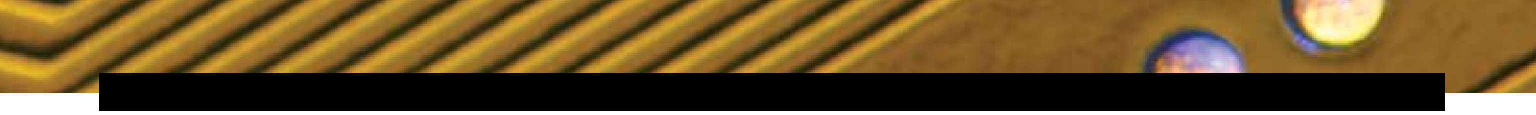
As we have seen, codes play an outstanding role in a CDMA system as GPS and Galileo are. But what does it mean to say that a code is good or bad, better or worse? To answer this question we have to talk first about pseudorandom noise, because a good code will be the one that best fulfils the characteristics of PRN.

In cryptography, pseudorandom noise refers to a signal that appears similar to RF noise and satisfies one or more of the standard tests for statistical randomness. This signal seems on observation to lack a definite cyclical pattern but, in fact, does follow a deterministic pattern that repeats itself eventually.

This is of great importance, as we've already pointed out, because the random sequences not only have to look as "random" as possible but must also be reproducible. In other words, a PRN code is one that has a spectrum similar to a random sequence of bits but is deterministically generated.

For most of the PRN codes, except the "random" or memory codes that will be discussed later, we need a pseudorandom number generator (PRNG). The PRNG is an algorithm that generates a sequence of numbers that are not truly random, but have very long periods.

Even more important than knowing the desired properties we want our codes to have is keeping in mind the limitations of our approach. As John von Neumann (1951) memorably stated, "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."



So, our task is to develop codes that appear as "random" as possible, but at the same time we need to have a way to generate them and reproduce them — an apparent contradiction in terms. Indeed, a very careful mathematical analysis is necessary to have any confidence that a PRNG does really generate numbers that are sufficiently "random", as R. Matthews and M. Luby have shown in their articles listed in the Additional Resources section at the end of this column.

Coming back to the inherent nonrandomness of the sequences generated by a PRNG, one can easily imagine that since PRNGs are run on a deterministic computer — in contrast to quantum computers — we need to use a deterministic algorithm to generate the PRN sequences. In consequence, the output of any computer with finite memory will inevitably have the property of periodicity, and, as we have emphasized at several points already, random codes cannot be periodic by definition.

PRNGs: A Brief History

The first works on computer-based PRNGs were published in 1946 by John von Neumann, who proposed an approach for generating PRN codes, known as the "middle square method." The idea of this method is as follows: take any number, square it, remove the middle digits of the resulting number as your "random number," then use that number as the seed for the next iteration.

For example, squaring the number "1111" yields "1234321," which can be written as "01234321," an 8-digit number being the square of a 4-digit number. This produces "2343" as the "random" number. Repeating this procedure gives "4896" as the next result, and so on.

The main problem of this method is that all sequences repeat themselves and some very quickly. Von Neumann was aware of this, but nonetheless he found the approach sufficient for his purposes. Indeed, he judged hardware random number generators unsuitable, because without being able to record the generated output at that time, they could not be tested for errors later.

The longer the codes, the better the properties present, but the price to pay is that long integrations are needed to find the correct delay between the satellite signal and the receiver replica.

The middle-square method has been improved upon for most purposes by more elaborate generators that produce pseudorandom sequences that are uniformly distributed by any of several statistics tests. Common classes of these algorithms include linear congruential generators, lagged Fibonacci generators, linear feedback shift registers (LFSRs), and generalized feedback shift registers. Recent instances of pseudorandom algorithms include Blum Blum Shub, Fortuna, and the Mersenne twister, this last one with a colossal period of 2^{19937}-1 iterations.

Another important point is that GNSS mass market applications require receivers that are easy to implement. This explains why the feedback shift register approach is still the most important procedure to generate pseudorandom sequences. The shift register approach presents the advantage that only the taps of the register have to be saved in memory because the different outputs are generated using the values of the taps according to a generation algorithm.

When GPS was designed for the first time, memory chips were not as cheap as they are today and thus the shift register approach was the easiest to implement in terms of memory. With the years, the memory capacities of microprocessors have improved, but to keep backwards compatibility the approach has been retained for the current existing codes. Today, memory capacity is no longer a problem, as can be seen with the memory-random codes approach followed by Galileo, which saves all the codes in memory is not so problematic.

Moreover, very long codes, in spite of their better properties would require very long integrations to find the correct delay between the satellite signal and the receiver replica, which would not be affordable for most of the applications.

Moreover, as we observed earlier, in order to improve the randomness of a set of codes, very long sequences are needed. The longer the codes, the better the properties present, but the price to pay is that long integrations are needed to find the correct delay between the satellite signal and the receiver replica, which would not be practical for most of the applications.

PseudorandomNoiseCodes

Now that we have seen the broad palette of algorithms that exist to generate pseudorandom sequences, we will analyze the properties of the most commonly used codes in CDMA systems, paying special attention to those that GPS and Galileo use now or will use in the near future.

Because codes comprise a very wide field, only some of the most popular sequences are listed here, and only the first six families will be described in detail in this article. Of special interest, then, to CDMA-based systems are the following PRN codes:

- Maximal length sequences or m-sequences
- Gold Codes
- Kasami Codes
- Weil Codes
- Random Codes – Memory Codes
- Bent Codes and Bent-function Sequences
- Barker Codes
- GMW Sequences
- Hadamard-Walsh Codes
- Rudin-Shapiro Sequences
- Golay Codes
- No Sequences
- Kronecker product Sequences
- Modified Jacobi Sequences
- Zero Cross Zones Sequences

Optimal PRN Code Selection. Selecting the best code is synonymous with selecting the code that performs best when measured against a metric considered to represent the "goodness" of a code.

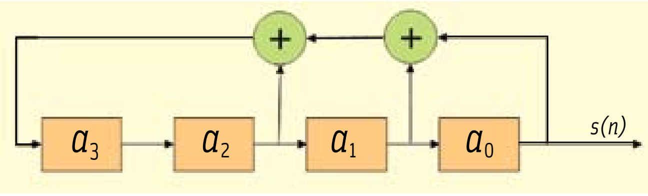


FIGURE 3 Feedback shift register representation

This is not an easy task, as the development of the Galileo codes described in the article by F. Soualle et al. has shown (see Additional Resources).

Indeed, the goodness of a code should not depend on receiver implementations, because the codes designed today will be transmitted for several decades, and it is impossible to predict changes in receiver implementation for this long period of time.

Additionally, depending on the targeted application, some properties are more important than others. For example, the autocorrelation is more important than the crosscorrelation for some applications and exactly the opposite happens in other applications.

Thus, since designing codes optimized for all the potential applications of GNSS is practically impossible, using a code-centric metric is more appropriate. This is the reason why the Welch bound has gained importance in recent years as a suitable metric for evaluating PRN codes.

The Welch lower bound is defined in the article by L. Welch (see Additional Resources) as

$$\theta_{Welch} = n\sqrt{\frac{M-1}{Mn-1}}$$

It determines the theoretical mininum of the maximum value of crosscorrelation that can be obtained for a code length n within a set of M codes. This expression can be further simplified when the number of sequences is relatively high, as it is the case in any GNSS application. In this case, the Welch Bound can be approximated to $\theta_{Welsh} \approx \sqrt{n}$. More accurate expressions on this bound have been obtained in work described by Tang X.H. et al.

For the optimization of the Galileo codes, various metrics (most of them are based on the Welch Bound) were employed to account for the different users Galileo will be targeting in the future, as Soualle discusses in detail. Additionally, Soualle et al. analyzed the code performance during the signal acquisition and tracking phases separately.

Indeed, most of these metrics include the Welch bound in their expressions and are based on the concepts of autocorrelation and crosscorrelation. For example, one metric examines the autocorrelation properties of a code p of length n: $(a_i)_{i=1}^{n},\ a_i \in \{-1,1\}$ which is defined as

$$AC_p(l, f_{offs}) = \frac{1}{n}\sum_{k=0}^{n-1}(a_k)_p\,(a_{k-l})_p\, e^{2\pi j\frac{f_{offs}}{f_s}k}$$

where

n code length,

a_k k – th code chip,

f_{offs} Doppler frequency offset,

f_s sampling frequency.

Equally, the crosscorrelation within a set of M codes $\left((a_k)_{k=1}^{n}\right)_{p=1}^{M},\ a_k \in \{-1,1\}$ between code p and q, $CC_{p,q}(l, f_{offs}), p, q \in \{1,..., M\}$, is defined as

$$CC_{p,q}(l, f_{offs}) = \frac{1}{n}\sum_{k=0}^{n-1}(a_k)_p(a_{k-l})_q\, e^{2\pi j\frac{f_{offs}}{f_s}k}$$

Autocorrelation and crosscorrelation are two figures that contain a lot of information about the code-properties of a family. For the optimization of GPS L1C codes, similar metrics are expected to have been considered.

Furthermore, other metrics have also shown to be good figures to identify good codes. The merit factor studied in the article by S. J. MacMullan (see Additional Resources), the anti-jamming robustness we will see when we talk about Bent codes, and all the works on sequences with large zero correlation zones (ZCZ) show promising fields that are still to be explored by GNSS researchers.

#feedback taps m	Codelength $n=2^m-1$	# m-sequences
13	8191	630
14	16383	756
15	32767	1800
17	131071	7710

TABLE1.Numberofm-sequencesforagiven shift register length

Code Types

Let's examine more closely now some of the leading codes used, or considered for use, in new GNSS signals.

Maximum Length Sequences. Also called m-sequences or n-sequences, maximum length sequences (MLS) are pseudorandom binary sequences generated using maximal linear feedback shift registers. M-sequences owe their name to the fact that they can be reproduced by a shift register with m taps resulting in a maximum length of $2^m - 1$ chips. Maximum length sequences are spectrally flat, with the exception of a zero continuous term.

M-sequences also constitute the basis for more complex structures such as the Gold codes that will be described next. We should underline the fact that every particular code structure generated using a PRNG is based in general on a limited number of primary sequences.

Using these basics, the corresponding code family is achieved by manipulations, that is, a shift and add in most cases. Additional randomness can be gained by adding various m-sequences of differing lengths and/or short-cycling them to obtain the desired length (truncated codes) as is the case with GPS L5 and L2. Given the fact that m-sequences can be implemented inexpensively in hardware or software, and relatively low-order feedback shift registers can generate long sequences, they are the basis for most of the codes used nowadays for GNSS.

Generation of m-sequences. As an example, Figure 3 shows an MLS generating system with four feedback taps. Any generating system of this type is described by a primitive polynomial that depends on the connections shown in the figure.

The number of m-sequences that exist for a given register length grows very quickly, making it extremely dif-

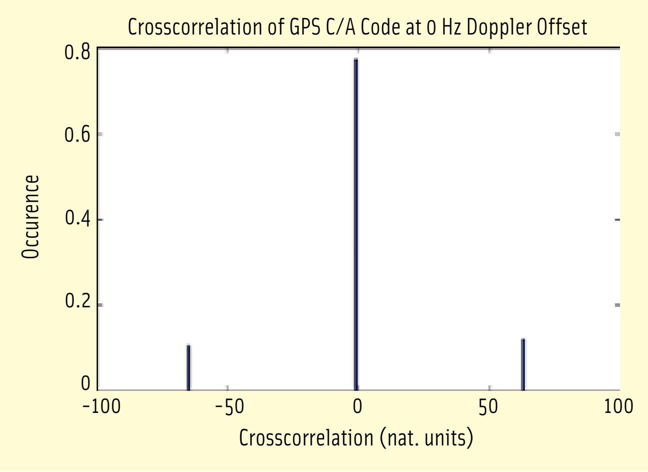


FIGURE 4 Crosscorrelation of GPS C/A codes for 0 Hz Doppler

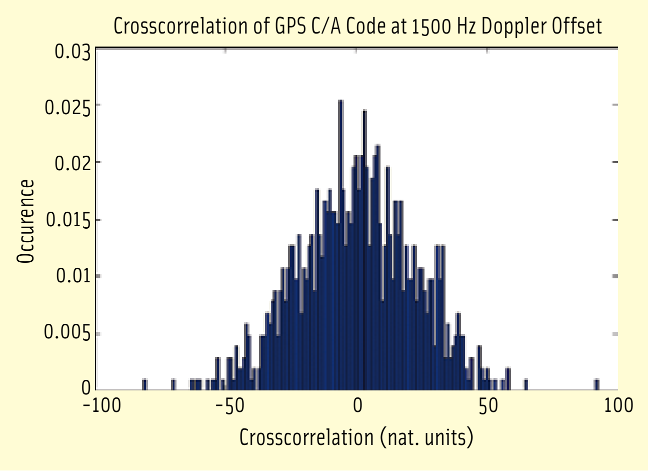


FIGURE 5 Crosscorrelation of GPS C/A codes for 1500 Hz Doppler

ficult to find the optimal one. Table 1 shows the number of m-sequences that exist with feedback taps from 13 to 17.

Because MLS are periodic and shift registers cycle through every possible binary value, registers can be initialized to any state, with the exception of the all-zero vector. This is what is called the initialization vector. In the case of GPS we can see this in the signal-in-space interface control document (SIS ICD), where every satellite is identified by a different initialization vector or delay.

Properties of maximum length sequence. The properties of the m-sequences were formulated by S. Golomb in his text *Shift Register Sequences*. These include

- *Balance Property.* The number of 1's in the sequence is one greater or equal to the number of 0's in the sequence.
- *Run Property.* This means that of all the "runs" in the sequence of each type, one half of the runs are of length 1, one quarter of the runs are of length 2, one eighth of the runs are of length 3, and so on. A "run" is a sub-sequence of 1's or 0's.
- *Correlation Property.* The autocorrelation and crosscorrelation of the m-sequence is periodic and binary valued.
- Maximum length sequences are related to the Hadamard transform.

Gold Codes

Because the C/A codes used in the open GPS L1 signal are based on Gold codes, this is the most popular type of codes in the GNSS community today. Gold codes are named after their inventor Robert Gold, who introduced them in two articles he published in 1967 and 1968 in the *IEEE Transactions on Information Theory.*

A Gold code family is based on XOR addition of two m-sequences of identical length n with an autocorrelation of the resulting code that consists beside the main peak of the three values

$$\theta_c(t) = \begin{cases} -1 & \text{or} \\ -t(m) & \text{or} \\ t(m)-2 \end{cases}$$

where $t(m) = 1 + 2^{\text{floor}(0.5\cdot(m+2))}$ with the number of feedback taps m and c denotes the XOR summation of the two m-sequences.

Every combination of m-sequences that holds the above criterion of a four-valued autocorrelation function after XOR-ing them is called a preferred pair. Obviously, the number of preferred pairs for a given number m of feedback taps is limited.

With the XOR addition of a preferred pair, a first Gold Code is generated and a whole code family can be obtained by adding the two sequences in their various phases. Thus the overall size of the code family is n+1 (two codes of the preferred pair and n-1 codes by adding them cyclically shifted), and it shows a three-valued crosscorrelation function in cases where no Doppler frequency offset is considered:

$$\theta_{c_i,c_j}(t) = \begin{cases} -1 & \text{or} \\ -t(m) & \text{or} \\ t(m)-2 \end{cases}$$

where m is the number of feedback taps and c_i,c_j denotes the combination of codes selected from the Gold code family.

Additionally the XOR operation of two Gold codes is another Gold code in some phase. The famous GPS C/A Gold code is based on LFSRs of order 10. Figures 4 and 5 show that the three-valued crosscorrelation property just holds for 0 Hz Doppler frequency offset mentioned earlier.

Kasami Codes

Codes in the small Kasami set fulfill many desired properties, such as having optimal crosscorrelation values touching the Welch lower bound.

The procedure used to build the small Kasami set is as follows: Let m be an even integer and u an m-sequence of period n=2^m-1. Starting with this sequence u, we obtain a decimated sequence $u[q]$ by selecting every q-th chip of u until a periodic sequence is obtained. This will happen at least after n elements.

If we work now with $u[q]$ being $q = 2^{m/2}+1$ and m being the degree of the sequence u, then the decimated sequence $u[q]$ is periodic with $2^{m/2}-1$ and, consequently, q-times repeating of $u[q]$, which leads us to a new sequence that we call w=$u[q]$. Then the small set of Kasami codes is obtained by XOR adding u and cyclically shifted versions of w:

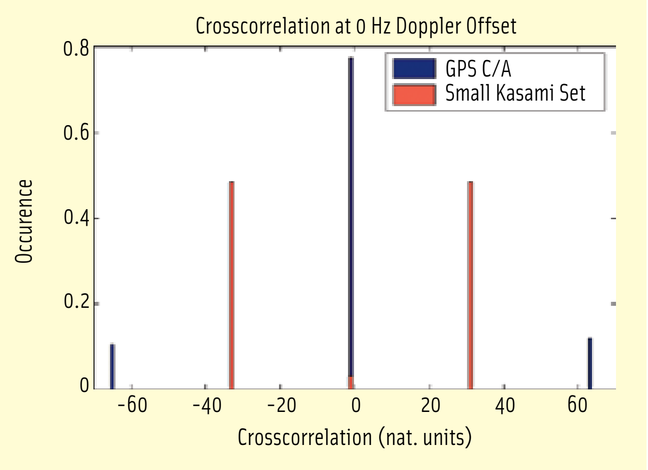


FIGURE 6 Crosscorrelation of the Small Kasami set for 0 doppler offset in natural units

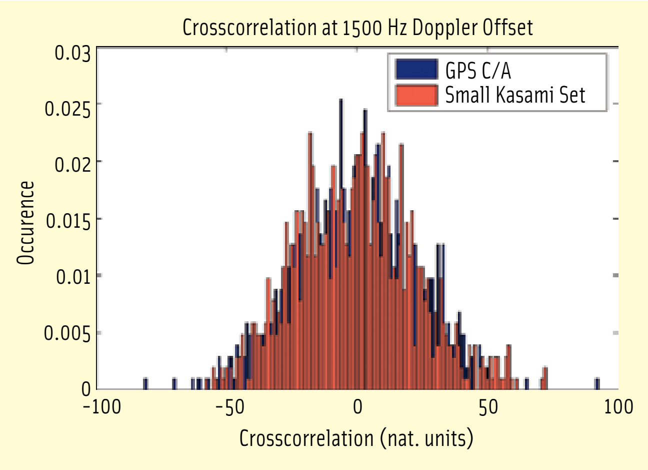


FIGURE 7 Crosscorrelation of the Small Kasami set for 1500 doppler offset in natural units

$$K_s(u)=\left\{u, u\oplus w, u\oplus Tw, u\oplus T^2 w,\ldots,u\oplus T^{2^{m/2}-1}w\right\}$$

where $\oplus$ represents the modulo 2 addition (XOR) of the vectors *u* and shifted versions of *w*.

This formulation reveals that the number of codes $\left(2^{m/2}+1\right)$ in the small set of Kasami is obviously very limited due to the repetition of *u*[*q*] within the sequence *w*.

The maximum crosscorrelation within the small set of Kasami codes shows optimal properties, as the crosscorrelation just consists of the three values

$$\theta_{c_i,c_j}(t)=\begin{cases}-1 & \text{or}\\ -2^{m/2}-1 & \text{or}\\ 2^{m/2}-1 & \end{cases}$$

where *m* refers to the number of feedback taps of the m-sequence and c_i,c_j denote the combination of codes within the code family.

For an even number of taps *m* we can get a code family of $M=2^{m/2}+1$ with an overall maximal absolute crosscorrelation of $\theta_{\max}=2^{m/2}+1$. The small set of Kasami codes can be shown to touch the Welch Bound asymptotically.

Figures 6 and 7 show a comparison of the crosscorrelation function between the GPS C/A codes and a small set of Kasami codes with the C/A codes' first m-sequence used as origin. With a maximum absolute crosscorrelation of 33 for the sample of the small set of Kasami codes shown here, the Welch bound of 31.48 is almost reached in the case of 0 Hz Doppler frequency offset.

The hardware implementation of Kasami sequences may look very complicated at first glance because a decimation process requires much faster clockings. However, the decimated sequence *u*[*q*] is by itself an m-sequence of order *m*/2, and the implementation complexity is thus reduced.

Moreover, the large set of Kasami Codes is an enhancement of the small set of Kasami codes as well as of the Gold codes. For its generation we use as basis sequences the two m-sequences that were used for generation of the Gold codes and the decimated sequence *w*=*u*[*q*] from the small set of Kasami codes.

The entire large set of Kasami codes can be generated as $c = u\oplus T^i v\oplus T^j w$ with *u*, *v* being a preferred pair of m-sequences and *w* being the decimated version of one of the two m-sequences, as was introduced in the small set of Kasami codes.

Now within the large set of Kasami codes we can clearly identify a number of special subsets:

- the two m-sequences that form the preferred pair
- the Gold Codes that can be created using these m-sequences
- the small set of Kasami Codes that can be obtained by combining one m-sequence with its decimated version *w* (here the second m-sequence is blanked)

The crosscorrelation function within the large set of Kasami codes is five-valued in the worst case and three-valued for the special cases of the Gold codes' respectively small set of Kasami Codes:

$$\theta_{c_i,c_j}(t)=\begin{cases}-1 & \text{or}\\ \pm 2^{m/2}-1 & \text{or}\\ \pm 2^{(m+2)/2}-1 & \end{cases}$$

where *m* refers to the number of feedback taps of the m-sequence and c_i,c_j denote the combination of codes within the code family. (See Figure 8.)

As we see, Kasami codes have very good properties regarding crosscorrelation but present a significant problem in that the small Kasami set is too small to be useful. This was, in fact, one of the drivers during the optimization of the E1 OS codes as the article by Soualle et al discusses. Indeed, Galileo needs 100 codes and GPS will have around 420 as can be seen in the respective SIS ICDs cited in Additional Resources.

Weil Codes and Legendre Sequences

Weil Codes are named after André Weil and will be used in the future GPS L1C. Weil codes are based on Legendre sequences; so, we will discuss the latter sequences first.

Legendre sequences are studied in several articles cited in the Additional Resources (Kitabayashi, S. et al;

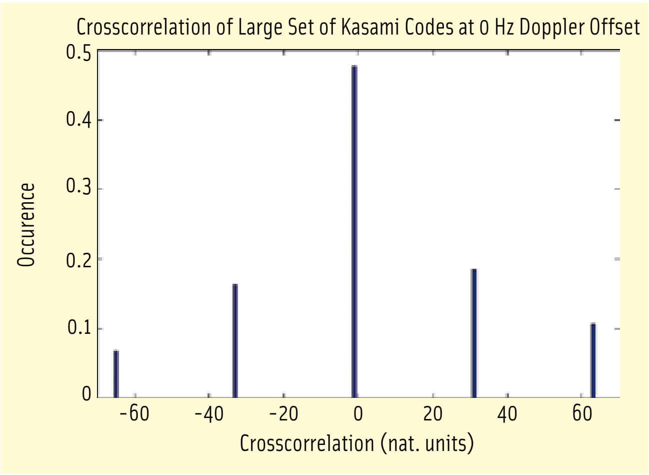


FIGURE8CrosscorrelationofLargeSetofKasamiCodewithoutDoppler Offset.

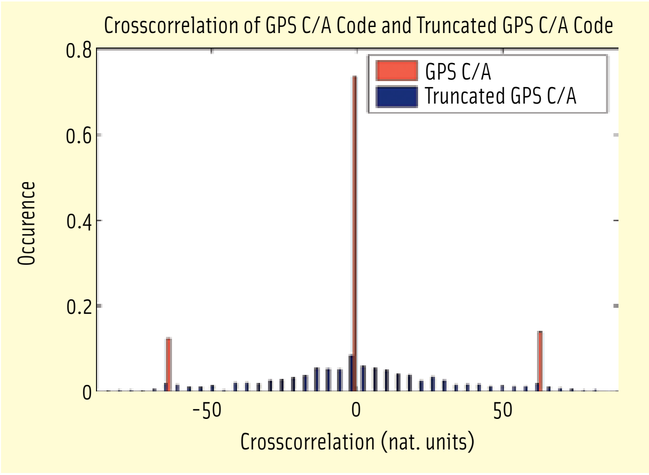


FIGURE9CrosscorrelationofGPSC/ACodeandcrosscorrelationofGPS C/A Code truncated by the last chip

Hoholdt, T. et al; Paterson, K.G.; Ding, C. et al; and Green, D.H. et al). These sequences are based on the quadratic residue of a prime.

Compared with other sequences like Gold codes, Legendre sequences are characterized by being based on prime numbers. While Gold codes must be of length 2^m-1, Legendre sequences are of length prime. This is interesting because the density of prime numbers within the set of natural numbers is higher than that of 2^m-1.

For a prime number L and an arbitrary positive integer a ($a<L$), we say that a is the quadratic residue (qr) of L if the equation x^2 mod $L = a$ has a solution x. We can prove whether a is a quadratic residue or not by computing the value of the expression $f(a) =$ $a^{(L-1)/2}$mod$L$.

Indeed this expression can only take values +1 (if a is a quadratic residue of L) and -1 (if a is not a quadratic resideue of L) and the two-valued random Legendre sequence is formed with it in the following manner:

$$[f(1)\ \ f(2)\ \ \ldots\ \ f(L-1)]$$

The obtained sequence has the interesting properties of having period L-1 being balanced and having the symmetrical relation on the centre of the sequence

$$f(k) = (-1)^{(L-1)/2} f(L-k)$$

with

$$(L-1)/2 \le k \le L-1$$

Another way of generating Legendre sequences is based on the fact that binary Legendre or quadratic residue sequences exist for all lengths L that are prime. They can be constructed using the Legendre symbol (i/L) which is defined as:

$$\left(\frac{i}{L}\right) = \begin{cases} 1 & \text{if } i \text{ is a qr mod } L \\ -1 & \text{otherwise} \end{cases}$$

Then, a Legendre sequence $a_0, a_1, a_2,\ldots,a_{L-1}$ is formed by writing

$$a_i = \left(\frac{i}{L}\right) \text{ for } 1 < i < L-1$$

which gives rise to two classes of Legendre sequences:

- Class 1: L=3mod4: The periodic autocorrelation function $\theta_a(i)$ takes values

$$\theta_a(i) = \begin{cases} L & \text{for } i = 0 \\ -1 & \text{otherwise} \end{cases}$$

- Class 2: L=1mod4. For this case

$$\theta_a(i) = \begin{cases} L & \text{for } i = 0 \\ -3 & \text{for } i \text{ a qr mod } L \\ 1 & \text{for } i \text{ a qnr mod } L \end{cases}$$

The XOR-addition of a Legendre sequence u with a shifted replica of itself results in the so-called Weil Code W.

$$W(u) = \left\{u \oplus Tu, u \oplus T^2 u, \ldots, u \oplus T^{\text{floor}(L/2)} w\right\}$$

The Weil Codes used for L1C are based on Legendre sequences of length 10223 since this is the closest prime to the desired code length of 10 milliseconds (10230 chips) that GPS L1C will have. To reach the 10230 chips length, a sequence of 7 chips (i.e., [0 1 1 0 1 0 0]) is inserted at a well-defined position within every Weil Code.

This position is referred as the Weil index.

Random, Memory Codes

"Random" codes, also known as memory codes in the literature, will be the ones that Galileo will use for the E1 Open Service (OS) and E6. As it has been shown, all codes present lengths 2^n–1 when they are based on an LFSR and a prime number for the Legendre codes.

At first glance one might think of the possibility to generate codes of any length by short cycling some of the codes we have discussed so far, given that they present very good properties. The problem is that, in fact, the truncation or expansion of these codes by even a single chip completely destroys their fine auto- and crosscorrelation properties as can be seen in Figure 9.

The idea of the patented random codes presented by J. Winkel in a 2006 filing is to generate a family of codes that fulfills the properties of random noise as well as possible for a given code length. The codes can be driven to fulfill special properties such as balance and weakened balance, where the probability of 0's and 1's must not be identical but within a well-defined range, or the autocorrelation sidelobe zero (ASZ) property. This latter ASZ (see Figure 10) guarantees that the autocorrelation values of every code correlate to zero with a delayed version of itself, delayed by one chip.

The plain number of choices to set the 0's and 1's for the whole code family is with 2^{nM} (n referring to the code length and M to the number of codes) unimaginably high. Even if doubled codes as well as codes with periodicity fault are excluded, the dimension of the problem is still huge. Consequently, special algorithms have to be applied to generate random codes efficiently (minimizing a cost function).

One possible implementation is the use of *genetic algorithms* that follow the principle of evolution and mutations, according to the Darwinist principle of the "survival of the fittest". Thus, starting with an initial set of codes or, if we stick to the biology notation, starting with an initial population, the codes or individuals that show the worst performance according to our selected figure of merit are chosen and eliminated or replaced by new ones.

Continuing with a smaller set of codes is the most extreme way, but the rule that is applied most often is to allow mutations within the code until a better code is found. A mutation must be understood in this context as a random flip of a number of chips within the code. If the mutated code shows better properties than the original one, the mutation is accepted, otherwise the mutation is rejected and new bits for flipping are randomly selected.

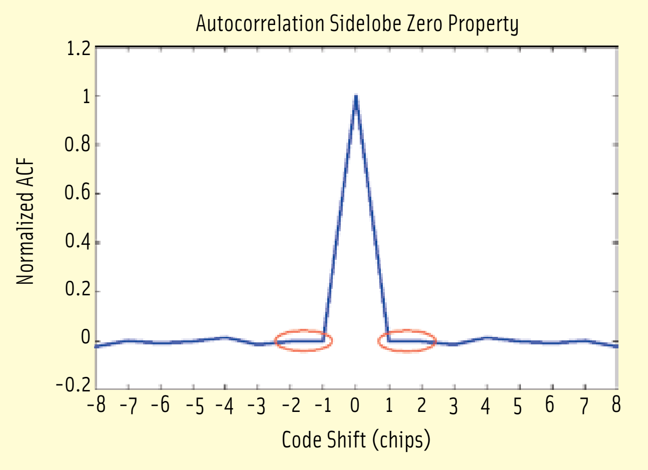


FIGURE 10 Autocorrelation properties of a random code with ASZ

Random codes, also known as *memory* codes are, despite their promising name, not truely random. As we saw in the introduction, no true random codes can be implemented with a finite length, but because they aspire to reach the best possible pseudorandom behavior for a given length, the term "random" is not completely wrong.

Random codes will be used for the first time in Galileo E1 OS und E6. Interest in them is growing because today memory chips can be produced ever more cheaply. Memory codes are unlike LFSR-generated codes in which only a short memory is needed to save the taps of the shift register and an algorithm runs continuously to obtain the code output at any moment. Instead, memory codes have the complete sequence saved in memory and only need to be "read".

The disadvantage of random codes for receiver manufacturers then is that more memory is needed to have all the codes saved, because they do not have to follow any generation procedure. But, as we have already commented, the cost of memory units has fallen dramatically in the last few years, and the trend is expected to continue.

Bent Codes and Bent-Function Sequences

Bent function sequences are a family of nonlinear binary signal sets that achieve the Welch's lower bound on simultaneous crosscorrelation and autocorrelation magnitudes (J. Olsen (1982)). Given a parameter m with mod(m,4) = 0 the period of the sequences is 2^m -1, the number of sequences in the set is $2^{m/2}$ and the cross/auto correlation function has three values with magnitude lower or equal to $2^{m/2}$+1.

These new code sets have the same size and correlation properties as the small set of Kasami Codes, but they have important advantages for use in spread spectrum multiple access communications systems. First, the sequences are "balanced", which represents only a slight advantage. Second, the sequence generators are easy to randomly initialize into any assigned code and hence can be rapidly "hopped" from sequence to sequence for code division multiple access operation.

Most importantly, the codes are nonlinear in that the order of the linear difference equation satisfied by the sequence can be orders of magnitude larger than the number of memory elements in the generator that produced it. The equivalent linear span of these codes is bound above by

$$\sum_{i=1}^{m/4} \binom{m}{i}$$

The linear span of a sequence is defined as the minimum number of stages of a linear feedback shift register needed to generate the given sequence. A high equivalent linear span ensures that the code sequence cannot be readily analyzed by a sophisticated enemy and then used to neutralize the advantages of the spread spectrum processing.

Bent sequences present very interesting code linear span values, which offer a good metric to measure how robust a code is against jamming in spread spectrum systems. The span of the code should be several times the processing gain. Jammers cannot determine the linear recursion of the code in a short enough time to harm the SS transmission. In fact, linear SS codes are not acceptable for anti-jam spread spectrum systems. For more information on Bent sequence the following papers are recommended: R. Scholtz (1978), P. Kumar (1983) and J.-S. No (2003)

We summarize in Table 2 the properties of all the code families discussed at length here.

Conclusions

Codes are a fundamental element in any GNSS system. Indeed, the final performance a receiver will experience depends much on the quality of the

	Period	Size of Code Family	Maximum Correlation Value	Constraints
Gold Codes	2^m-1	2^m+1	$2^{\text{floor}(0.5 \bullet (m+2))}+1$	*
Small set of Kasami Codes	2^m-1	$2^{m/2}$	$2^{m/2}+1$	*, $\text{mod}(m, 2) = 0$
Large set of Kasami Codes	2^m-1	$2^{m/2}\left(2^m+1\right)$	$2^{(m+2)/2}+1$	*, $\text{mod}(m, 4) = 2$
Weil Codes	L	(L-1)/2	$1+4 \bullet \text{floor}\left(0.5L^{0.5}\right)$	$\text{mod}(L,2) = 1$
Bent Codes	2^m-1	$2^{m/2}$	$2^{m/2}+1$	$\text{mod}(m,4) = 0$

TABLE 2. Comparison between Golf Codes, Small and Large set of Kasami Codes, Weil Codes and Bent Codes. * Generating m-sequences have to be preferred pairs

Civil codes	Galileo	GPS
E1/L1	Random codes (E1OS)	Gold codes (C/A) Weil codes (L1C)
L2	-	m-sequences*
E5/L5	m-sequences	m-sequences**
E6	Random codes	-

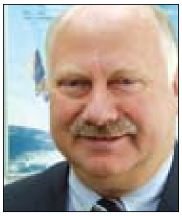
TABLE 3. Civil GNSS codes. *The same polynomial generator used for L2 CM and L2 CL with the difference that L2 CM is reset after 20 ms and L2 CL after 1.5 seconds. ** The different codes of the family are obtained employing different m-sequences and short-cycling.

selected family of codes. Gold codes and truncated codes have been the most used solutions in the past but in the last years with the optimization of GPS and the birth of Galileo radically different approaches with better properties have come into play. This is not a static field of study at all and a quick look in the literature shows that much work has been done and remains to be done.

As we have seen in this paper, optimizing codes is not an easy task. In fact, the desirable properties a family should present depend highly on the application the code is intended to serve. What use we will make of GNSS in the future is something that only time will tell, and thus the goodness of the codes for every certain application will definitely not be uniform.

As a summary, Table 3 shows the code families that will be used by Galileo and GPS in every band.

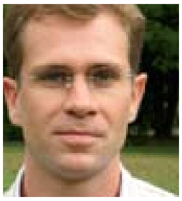
Authors



"Working Papers" explore the technical and scientific themes that underpin GNSS programs and applications. This regular column is coordinated by PROF. DR.-ING. GÜNTER HEIN.

Prof. Hein is a member of the European Commission's Galileo Signal Task Force and organizer of the annual Munich Satellite Navigation Summit. He has been a full professor and director of the Institute of Geodesy and Navigation at the University of the Federal Armed Forces Munich (University FAF Munich) since 1983. In 2002, he received the United States Institute of Navigation Johannes Kepler Award for sustained and significant contributions to the development of satellite navigation. Hein received his Dipl.-Ing and Dr.-Ing. degrees in geodesy from the University of Darmstadt, Germany. Contact Prof. Hein at <Guenter.Hein@unibw-muenchen.de>.

José-Ángel Ávila-Rodríguez is a research associate at the Institute of Geodesy and Navigation at the University FAF Munich. He is responsible for research activities on GNSS signals, including BOC, BCS, and MBCS modulations. Ávila-Rodríguez is involved in the Galileo program, in which he supports the European Space Agency, the European Commission, and the Galileo Joint Undertaking, through the Galileo Signal Task Force. He studied at the Technical Universities of Madrid, Spain, and Vienna, Austria, and has an M.S. in electrical engineering. His major areas of interest include the Galileo signal structure, GNSS receiver design and performance, and Galileo codes.



Stefan Wallner studied at the Technical University of Munich and graduated with a Diploma in techno-mathematics. He is now research associate at the Institute of Geodesy and Navigation at the University FAF Munich. Wallner's main topics of interest are the spreading codes and the signal structure of Galileo and also interference and interoperability issues involving GNSS systems.

Additional Resources

Von Neumann J., and A.S. Householder, G.E. Forsythe, and H.H. Germond, "Various techniques used in connection with random digits," in eds., Monte Carlo Method, National Bureau of Standards Applied Mathematics Series, 12 (Washington, D.C.: U.S. Government Printing Office, 1951), pp. 36-38

Matthews R., "Maximally Periodic Reciprocals," Bulletin of the Institute of Mathematics and its Applications 28, pp. 147-148, 1992

Luby M. (1996), "A definitive source of techniques for probably random sequences," Pseudorandomness and Cryptographic Applications, Princeton Univ Press, 1996

Soualle F., M. Soellner, S. Wallner S., J. A. Avila-Rodriguez, G.W. Hein, B. Barnes, T. Pratt, L. Ries, J. Winkel, C. Lemenager, and P. Erhard, "Spreading Code Selection Criteria for the Future GNSS Galileo," Proceedings of GNSS 2005, Munich 19-22 July 2005

Welch L., "Lower bounds on the maximum cross correlation of signals," IEEE Transactions on Information Theory, Vol. IT-20, No. 3, pp. 397–399, May 1974

Tang, X.H., and P.Z. Fang, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlation zone," Electronic Letters, Vol. 36, No. 6, pp. 210–218, March 2000

MacMullan S.J., and O.M. Collins, "A Comparison of Known Codes, Random Codes, and the Best Codes," IEEETIT: IEEE Transactions on Information Theory, 1998

IS-GPS-200: NAVSTAR GPS Space Segment/Navigation User Interfaces

Golomb, S., Shift Register Sequences, San Francisco, Holden-Day, 1967

Gold, R.), "Optimal binary sequences for spread spectrum multiplexing (Corresp.)," IEEE Transactions on Information Theory. Volume 13, Issue 4, Oct. 1967, pp. 619–621

Gold, R., "Maximal recursive sequences with 3-valued recursive cross correlation functions (Cor-

Working Papers *continued on pg 75.*

resp.)," IEEE Transactions on Information Theory. Vol. 14, Issue 1, January 1968, pp.154–156

Galileo SIS ICD 23/05/2006

Kitabayashi S., and T. Ozawa and M. Hata, "Property of the Legendre Subsequence" Singapore ICCSI ISITA, 1992

Hoholdt T., and H. E. Jensen, "Determination of the Merit Factor of Legendre Sequences," IEEE Transactions on Information Theory, Vol. 34, No. 1, January 1988

Paterson K.G., "New Binary Sequence Sets with Favourable Correlations" ISIT 1997, Ulm, Germany, June 29 – July 4, 1997

Ding C., and T. Helleseth, W. Shan W, "On the Linear Complexity of Legendre Sequences", IEEE Transactions on Information Theory, Vol. 44, No. 3, May 1998

Green D.H., and P.R. Green P.R., "Polyphase related-prime sequences", IEE Proc.-Comput-Digit. Tech, Vol. 148, No. 2, March 2001

Winkel J., Patent number WO2006063613, 22-6-2006, H04J13/04, H04B1/707, H04J13/02, H04B1/707

Olsen, J., and R. Scholtz and L. Welch, "Bent-function sequences", IEEE Transactions on Information Theory. Vol. 28, Issue 6, November 1982, pp. 858–864

Scholtz, R., and L. Welch and P. Kumar, "Group characters: Sequences with good correlation properties," IEEE Transactions on Information Theory, Vol. 24, Issue 5, September 1978, pp. 537–545

Kumar, P., Scholtz, R. (1983), "Bounds on the linear span of bent sequences," IEEE Transactions on Information Theory. Volume 29, Issue 6, Nov 1983 Page(s): 854 – 862

Jong-Seon No, Gang-Mi Gil, Dong-Joon Shin (2003), "Generalized construction of binary bent sequences with optimal correlation property, IEEE Transactions on Information Theory. Volume 49, Issue 7, July 2003 Page(s): 1769 - 1780