Codes: The PRN Family Grows Again

© iStockphoto.com/agencyby

Unlike most families that become more robust the more the members have in common with each other, pseudorandom noise families grow stronger the more different their sequences are to one another. This column introduces some new offspring from the familiar elements of GNSS and other radionavigation system codes.

STEFAN WALLNER, JOSÉ-ÁNGEL ÁVILA-RODRÍGUEZ
EUROPEAN SPACE AGENCY

Pseudorandom noise (PRN) sequences are an essential element of any radionavigation satellite system that is based on code division multiple access (CDMA) techniques. Indeed, these sequences enable a navigation receiver to distinguish one satellite from another.

A comprehensive introduction to CDMA, including its history in general and PRN sequences in particular, can be found in the Working Papers column by G. W. Hein *et alia* published in the September 2006 issue of *Inside GNSS*.

After the finalization of the Galileo PRN codes back in 2004 and the definition of the GPS L1C codes in about the same timeframe, additional attention to this very interesting field of research is now expected in the near future. In fact, not only additional CDMA-based signals will appear from GNSS satellites, but a steadily growing interest in ground based, continuously transmitting pseudolites can also be observed.

This interest will undoubtedly animate further research on high-performing sets of PRN codes with certain characteristics regarding code length and the number of codes to support design of the new signals to be provided by these systems. The New PRN Code Family introduced in this column could be one potential candidate for such systems because it offers a number of highly advantageous characteristics that we will analyze in this article.

System designers need to select the best codes according to some *figure of merit* (FOM) indicating the performance of the PRN code set. A large variety of FOMs can be imagined, and dedicated publications deal with this subject. See, for example, the paper by F. Soualle et alia referenced in the Additional Resources section near the end of this article.

The correlation function goes back to the *mean squared error* concept introduced by Carl Friedrich Gauss (1777–1855) and is without doubt one of the most widely used and most powerful means to characterize the performance of PRN sequences. It can measure the communality between different sequences of length N and is defined for 0-hertz Doppler frequency offset as

$$\theta_{u,v}(l) = \sum_{n=0}^{N-1} v(n+l)u(n)$$

where

$u(n)$ n-th chip of sequence u

$v(n + l)$ $n+l$-th chip of sequence v.

The correlation function shown by this equation is also referred to as *even correlation* because it does not account for a flip of the sequence within the integration period as might be induced due to a data or secondary code bit change. This article will address the issue of *odd correlations* later on. The objective of the following discussion is to introduce and mathematically derive the New PRN Code Family and characterize it in terms of correlation performance.

Generation of PRN sequences

Regarding the generation of PRN sequences, we can distinguish between two categories:

- PRN sequences, where the value of each chip of the sequence is based on a mathematical, closed form algorithm, and
- PRN sequences that result from a numerical optimization or selection process.

For the latter category, the individual chips of the PRN codes cannot be determined by applying a closed mathematical formula, while specific algebraic formulas can be given for the first category of sequences that result immediately in the PRN sequences.

Well-known PRN sequences that belong to this first category include

- Gold codes
- Kasami codes
- Weil codes
- Bent-function sequences
- No
- Gong/Paterson, and
- Z4 linear Family I and II.

Articles and papers referenced in the Additional Resources section discuss most of these in further detail.

These codes offer almost ideal auto- and cross-correlation properties for zero Doppler frequency offset. Unfortunately, they face the restriction that they can only be constructed for specific code lengths.

The PRN code length results generally from dividing the signal's chip rate and its corresponding symbol rate. For PRN sequences that are derived from closed analytical expressions, any deviation from the preset code length immediately results in a significant degradation in terms of increased cross-correlation and out-of-phase autocorrelation. For instance, any codes based on *linear feedback shift registers* (LFSRs), such as Gold codes and Kasami codes, can be set up for any length $N = 2^n - 1$ for integer values n that respect mod(n, 4) $\neq 0$.

In contrast to LFSR-based sequences, Weil codes can be constructed for any prime code length. This is a benefit because there are more prime numbers than lengths $N = 2^n - 1$, thus allowing for additional flexibility. Paterson or Gong sequences need to comply with a code length being the square of a prime number.

Obviously, the potential code lengths enabling the construction of prime length sequences significantly exceed the code lengths from which to choose when setting up LFSR-based sequences. This is further underlined in **Figure 1**, which shows that in a mathematical sense the prime numbers lie much denser in the natural numbers $\mathbb{N}$ than the numbers $2^n - 1$ for integers n do.

For $0 < N < 50{,}000$, a total of 5,133 prime numbers exist but only 48 prime squares, and LFSR-based sequences can only be set up for 15 different sequence lengths.

As already mentioned, any truncation or elongation of PRN sequences immediately results in a significant increase in auto- and cross-correlation as shown in the **Figure 2**. In this example, just the very last chip of 1,023-chip Gold codes — as they are used for the GPS C/A code signal — was deleted, leading to truncated Gold codes of length

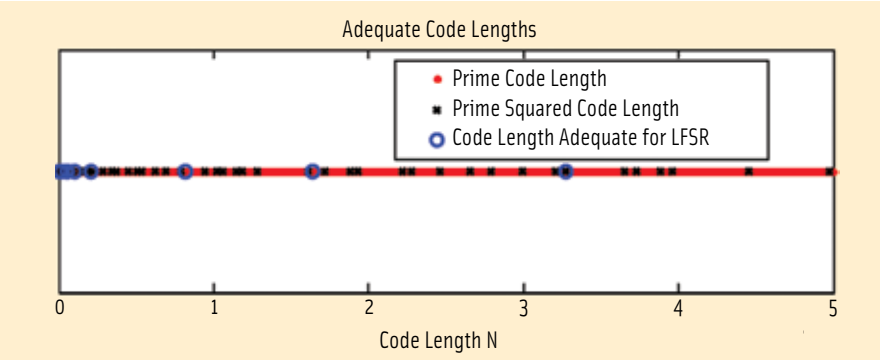

FIGURE 1 **Adequate code lengths for LFSR-based sequences, prime, and prime-squared length sequences**

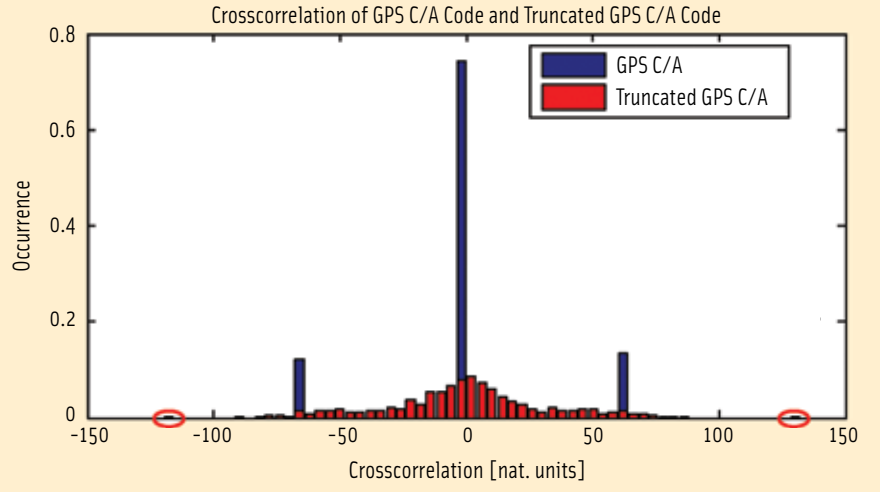

FIGURE 2 **Degradation of correlation performance after truncation**

1,022. While the cross-correlation for Gold codes of order 10 is bounded by -65 and 63, the correlation values of the truncated version spread out to -120 and 132 (indicated by the red ellipses in the figure), and are thus significantly worse.

Obviously, in many cases the requirements of the PRN code length as driven by the signal's chip rate and its symbol rate are not compatible with the available, analytically defined options for PRN code generation. In order to close this gap, some signal designs make use of truncation or elongation to come to the desired code lengths.

For instance a head/tail concept could be applied as it was under early consideration for the Galileo E5 PRN codes. In order to achieve the required code length a full run of a LFSR-based sequence (representing the head) needs to be concatenated with a truncated LFSR-based sequence (representing the tail). Similar concepts can be also be found at GPS L1C, where Weil sequences with a length of 10,223 chips are complemented by a well chosen 7-chip pad (inserted into the Weil sequence at a specific index), and in Compass signal designs.

In order to allow for maximum flexibility regarding the PRN code length, numerical generation and optimization methods have been identified. Genetic algorithms can be used to construct random codes of any desired length, optimized for any potential FOM imaginable, and implemented during the design of the PRN sequences. (For further details, see the patent application by J. Winkel listed in Additional Resources.)

Alternatively, signal designers can make use of chaotic algorithms to set up the PRN sequences displaying properties that are as close as possible to random sequences, as described in the patent application publication by M. Hadef *et alia*.

The new code family that we shall define next belongs to the first category, with its sequences constructed based on closed-form algebraic formulas.

Generation of New Family with Even Code Length

We introduce next a new code family that can be constructed for code lengths N that follow the form, $N = p - 1$, where p refers to any prime number larger than 7. So, any sequence contained in the new code family results in an *even* length. This is of particular interest because most of the code families that are generally known in the literature are constructed from closed formulas that include a sufficiently large number of codes with the property of having an *odd* length. This is indeed the case for LFSR-based sequences as well as for Weil-codes.

The new code family can be derived from a single sequence in contrast to, for example, Gold codes and Kasami codes. Indeed, these require two appropriately selected *maximum length sequences* (M-sequences) that form the basis from which to derive the full code family.

M-sequences can be generated using maximum LFSR, and they produce every binary sequence that an LFSR can cycle through except the all-zero state. In this way an n-stage LFSR is capable of generating a binary sequence of length $2^n - 1$, if the feedback taps are chosen properly, and the resulting M-sequence shows a spectrally flat autocorrelation function.

Two M-sequences showing specific cross-correlation properties are referred to as a *preferred pair* and form the basis from which to derive Gold or Kasami Codes (A good overview on M-Sequences, Gold Codes, and Kasami Codes can be found in the previously referenced Working Papers column by G. W. Hein *et alia* and in *Spread Spectrum Systems for GNSS and Wireless Communications*, authored by J. K. Holmes.)

As with the new family of PRN codes proposed here, the Weil codes are just based on a single generative sequence. A method to generate binary sequences has been proposed independently by V. M. Sidelnikov and A. Lempel *et alia* (see Additional Resources). The binary sequence derived from their methods will serve as a generative one for our new PRN code family. From here on, this column will refer to these as *SLCE sequences*.

SLCE sequences are based on primitive root elements. A short definition of primitive roots is as follows:

> If m is a positive integer, the congruence classes coprime to m form a group with the multiplication modulo m as the internal operation; it is denoted by $Z_m^\times$ and is called the group of units (mod m) or the group of primitive classes (mod m). A generator of this cyclic group is called a **primitive root** modulo m.

To demonstrate how this works, we take for illustration purposes the task of finding a primitive root for $m = 14$. Consequently, the group of all co-prime numbers with respect to $m = 14$ is denoted as $Z_m^\times$ and is shown to be formed by $Z_m^\times = \{1,3,5,9,11,13\}$. For an integer number pr to be primitive root modulo of 14, we now need to prove that the function

$$g: Z_{14} \rightarrow Z_{14}^\times : g(pr, i) = \mathrm{mod}\left(pr^i, 14\right), i \in Z$$

is surjectiv onto $Z_m^\times$, i.e., all elements of $Z_m^\times$ can to be "obtained" by the function g. As an example, we will next test whether 3 or 9 is a primitive root modulo 14. This is depicted in Table 1, where all results are taken modulo 14.

As we can see from the table, the integer powers of 3 modulo 14 generate all elements of $Z_m^\times$ while, for instance, 5 is not obtained by any power of 9 modulo 14. Thus we can conclude that 3 is a primitive root modulo 14 while 9 is no primitive root modulo 14. Further analysis shows that only the numbers 3 and 5 are primitive root elements modulo 14.

For the generation of the following sequences, it is interesting to know how many different primitive root elements can be determined for a specific integer m. In order to do so, we recall the totient function $\varphi(m)$ that goes back to the Swiss mathematician Leonhard Euler (1707–1783) plays an important role. Euler's toti-

pr	*g (pr,1)*	*g (pr,2)*	*g (pr,3)*	*g (pr,4)*	*g (pr,5)*	*g (pr,6)*	*g (pr,7)*
3	3	9	13	11	5	1	3
9	9	11	1	9	11	1	9

TABLE 1. Test for primitive root modulo 14

ent function determines the order of $Z_m^{\times}$ or, in other words, the number of *coprime* elements for an integer m and is defined as

$$\varphi(m) = m\prod_{k=1}^{M}\left(1-\frac{1}{p_k}\right) \quad (1)$$

where p_k relate to the M prime factors that constitute the integer m. The following lines provide a short proof for equation (1).

For a prime number p_k there exist exactly $p_k - 1$ coprime elements. When setting the prime number to an exponent $e_k \in \mathbb{N}$, we can exactly identify the number of elements that are not coprime to ${p_k}^{e_k}$. These non–co-prime elements list to p_k, $2p_k$ $3p_k$,..., ${p_k}^{e_k-1}p_k = p_k$, and their number is exactly ${p_k}^{e_k-1}$. Consequently,

$$\varphi\left({p_k}^{e_k}\right) = {p_k}^{e_k} - {p_k}^{e_k-1} = {p_k}^{e_k}\left(1-\frac{1}{p_k}\right)$$

As any natural number m can be represented as

$$m = \prod_{k=1}^{M} p_k^{e_k}$$

with M prime factors p_k and corresponding orders e_k we finally result in

$$\varphi(m) = \varphi\left(\prod_{k=1}^{M}{p_k}^{e_k}\right) = \prod_{k=1}^{M}\varphi\left(p_k^{e_k}\right) = \prod_{k=1}^{M}{p_k}^{e_k}\left(1-\frac{1}{p_k}\right) = m\prod_{k=1}^{M}\left(1-\frac{1}{p_k}\right)$$

As shown in the text, *Elementary Number Theory*, authored by D. M. Burton, here exist exactly $\varphi(\varphi(m))$ incongruent primitive root elements modulo m if any primitive root element exists for m. If m equals a prime number p, this simplifies to $\varphi(\varphi(p)) = \varphi(p-1)$. **Figure 3** shows the number of primitive root elements that can be obtained for prime numbers p.

The identification of a primitive root element is the first and basic step for generating SLCE sequences. For the next step we need to form a set S defined as

$$S = \left\{pr^{2i+1} - 1\right\}_{i=0}^{k-1} \quad (2)$$

with

pr primitive root modulo p

p prime number

$$k = \frac{1}{2}(p-1)$$

which is actually half the desired code length.

The final SLCE sequence $u_{SLCE}(n)$ is defined for a delay n according to the following formula:

$$u_{SLCE}(n) = \begin{cases} +1 & \text{if } pr^n \in S \\ -1 & \text{else} \end{cases}, \quad 0 \le n < 2k \quad (3)$$

Elementary Number Theory identifies the autocorrelation side peaks for SLCE sequences for any primitive root elements to be given by

$$\theta_{u_{SLCE}}^{\text{Cat1}} \in \begin{cases} \{-2, 2\} & \text{if } k \text{ is odd} \\ \{-4, 0\} & \text{if } k \text{ is even} \end{cases} \quad (4)$$

However, depending on the selection of the primitive root element pr, an additional category of SLCE sequences can be identified for which the out-of-phase autocorrelation follows:

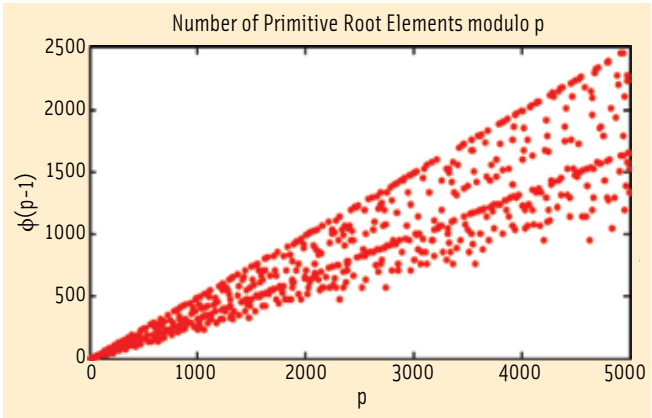

FIGURE 3 **Number of primitive root elements modulo *p***

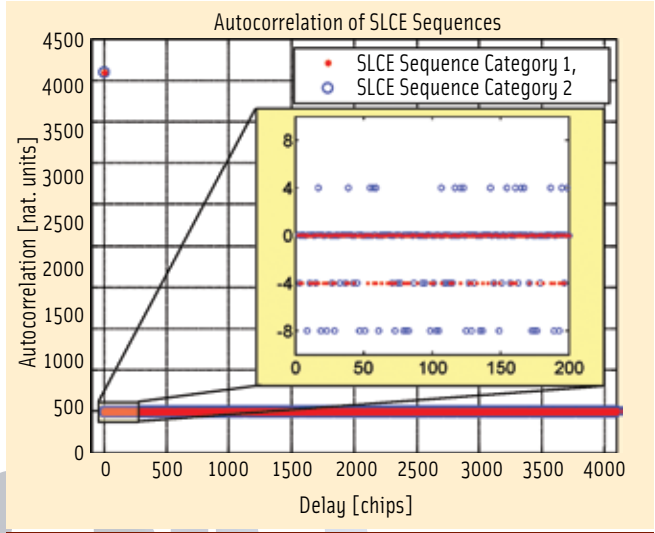

FIGURE 4 **Even autocorrelation of SLCE sequences**

$$\theta_{u_{SLCE}}^{\text{Cat2}} = \begin{cases} \{-6, -2, 2\} & \text{if } k \text{ is odd} \\ \{-8, -4, 0, 4\} & \text{if } k \text{ is even} \end{cases} \quad (5)$$

Based on this finding, we can identify the two following categories of primitive root elements pr^{Cat1} and pr^{Cat2} that lead to SLCE sequences offering slightly different autocorrelation properties:

$$pr \in pr^{\text{Cat1}} \Leftrightarrow \theta_{u_{SLCE}} = \theta_{u_{SLCE}}^{\text{Cat1}}$$
$$pr \in pr^{\text{Cat2}} \Leftrightarrow \theta_{u_{SLCE}} = \theta_{u_{SLCE}}^{\text{Cat2}} \quad (6)$$

For any prime number p, the number of primitive root elements is always even, and half of them lead to SLCE sequences with a Category 1 autocorrelation function while the other half results in SLCE sequences with a Category 2 autocorrelation function.

SLCE sequences of Category 1 show absolute balance; thus, the number of +1s in the sequence equals the number of -1s. For SLCE sequences of Category 2 the balance depends on k, as defined earlier. For an even k, the number of 1s exceeds the number of -1s by 2, while for odd k, there are two more -1s in the sequence than +1s.

The even autocorrelation functions of two SLCE sequences based on primitive root elements from set pr^{Cat1} and pr^{Cat2} of length N=4,092 are shown in **Figure 4**, and we can verify formula (4) as the autocorrelation side lobes adopt only values of either 0 or -4 or only either 4,0,-4 or -8.

Although the SLCE sequences show excellent autocorrelation performance, the cross-correlation between them proves just to be of a purely random nature. Indeed, it appears similar to the cross-correlation that would be obtained for any random and non-optimized sequences.

The text in the accompanying box introduces the approach that has been identified in order to derive from a single SLCE sequence a full set of PRN codes that not only show good autocorrelation performance but also are favorable with respect to their cross-correlation characteristics.

The new code family of even length offering ideal correlation performance can be constructed based on the following generation scheme. The i-th PRN sequence of this family is given by:

$$u^i = u_{SLCE} \oplus T^i u_{SLCE} \quad (7)$$

where

- u_{SLCE} relates to the generative SLCE sequence belonging either to Category 1 or Category 2, depending on the selection of the primitive root element,
- $\oplus$ to the element by element binary XOR addition and
- T^i indicates a cyclic shift of i chips.

The generation of the New PRN Code Family is depicted in **Figure 5**.

Depending on the primitive root element on which the generative SLCE sequence u_{SLCE} is based, two different categories of the new code family can be derived, namely, Category 1 and Category 2. Both categories of the new code family show excellent, but slightly different auto- and cross-correlation properties.

Properties and Performance of New Code Family

Several distinctive properties are associated with the new PRN code family, which we will characterize next. The performance of the code family will also be discussed in the following section.

Balance. The balance property *BAL* for the n-th PRN sequence is defined by the addition of the individual chips, i.e.:

$$BAL^n = \sum_{i=1}^{N} u_i^n \quad (8)$$

The balance of a PRN sequence follows the Golomb postulates for randomness with one FOM to characterize the randomness of any PRN sequence. In an ideal case the BAL FOM is as close to zero as possible. For the new code family the balance value of the balance property is closely related to the autocorrelation function of the generative SLCE sequence, as the balance for the n-th PRN sequence calculates to

$$BAL^n = \sum_{i=1}^{N} u^n(i) = \sum_{i=1}^{N} u_{SLCE}(i) \oplus T^n u_{SLCE}(i) = \theta_{u_{SLCE}}(n) \quad (9)$$

In consequence, it turns out that

$$BAL^{n,CAT1} \in \begin{cases} \{-2,2\} & \text{if } k \text{ is odd} \\ \{-4,0\} & \text{if } k \text{ is even} \end{cases} \text{ for category 1 codes} \quad (10)$$

$$BAL^{n,CAT2} = \begin{cases} \{-6,-2,2\} & \text{if } k \text{ is odd} \\ \{-8,-4,0,4\} & \text{if } k \text{ is even} \end{cases} \text{ for category 1 codes} \quad (11)$$

Thus, the balance criterion is close to be fulfilled in an ideal way. Moreover, the balance criterion is fulfilled ideally for subsets of Category 1 and Category 2 sequences.

Correlation Performance. As already mentioned, the auto- and cross-correlation performance is an essential metric by which to characterize the performance of PRN sequences as they are applied for CDMA systems.

We can consider the so-called Welch Lower Bound, or Welch Bound for short, to be the most applied theoretical limit when talking about the best correlation performance that a family of PRN codes can achieve. The Welch Bound indicates the minimum of the maximum achievable out-of-phase auto- and cross-correlation magnitudes. Indeed, no set of PRN sequences can result in maximum correlation magnitudes lower than the Welch Bound for any set of PRN sequences.

The article by L. R. Welch cited in Additional Resources provides a mathematical introduction and definition of the Welch Bound. For a set of K sequences each of length N, the Welch bound calculates as

$$\theta_{Welch} = N\sqrt{\frac{K-1}{KN-1}}. \quad (12)$$

Furthermore, we can easily see that, if only the code length N tends to infinity, the Welch bound simplifies to

$$\theta_{Welch} = \sqrt{N}. \quad (13)$$

The well-known Gold codes tend to approach the limit of the Welch bound for $N \to \infty$. The maximum auto- and cross-correlation sidelobes for a set of Gold codes of order n calculate to

$$\max\left|\theta^{Gold}\right| = 1 + 2^{\lfloor (n+2)/2 \rfloor} \quad (14)$$

Consequently, two categories of Gold codes can be identified, depending on whether n is odd or even, with different maximum correlation magnitudes:

$$\max\left|\theta^{Gold}\right| = \begin{cases} 2\left\lceil\sqrt{2^n-1}\right\rceil + 1 = 2\left\lceil\sqrt{N}\right\rceil + 1 & \text{for } \mathrm{mod}(n,4) = 2 \\ \left\lceil\sqrt{2\left(2^n-1\right)}\right\rceil + 1 = \left\lceil\sqrt{2N}\right\rceil + 1 & \text{for } \mathrm{mod}(n,2) = 1 \end{cases} \quad (15)$$

where $N = 2^n - 1$ represents the code length.

We will use this Gold code limit in order to next demonstrate the relative value of the new code families in terms of correlation performance. We should note that Gold codes are not available for an order of n being a multiple of 4 (i.e., mod(n, 4) = 0).

Coming back to the New Code Family as it was introduced in equation (7), any primitive root element can be used to derive

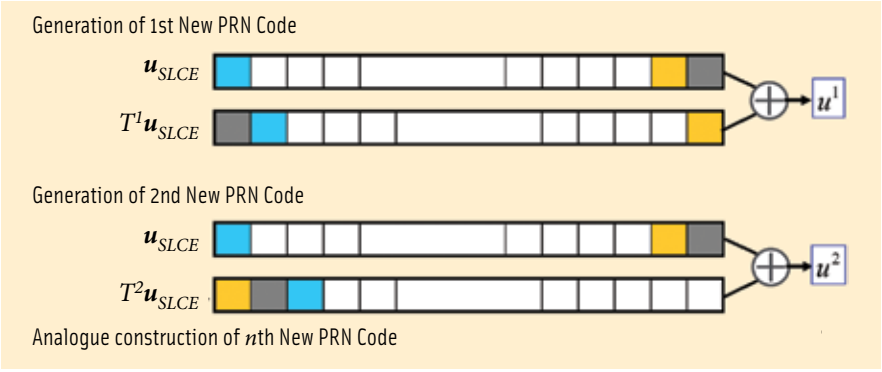

FIGURE 5 **Generation of the new PRN code family**

it. Depending on the selected primitive root element, two categories of SLCE sequences can be obtained and, consequently, two different categories of PRN code families also result, each of them showing slightly different, but still excellent correlation characteristics.

The two categories can also be distinguished by their corresponding maximum correlation magnitude:

$$\max\left|\theta^{New\,Code\,Family}\right| = \begin{cases} 2\left\lceil\sqrt{p-1}\right\rceil+4 = 2\left\lceil\sqrt{N}\right\rceil+4 & \text{for } pr \in pr^{CAT1} \\ 2\left\lceil\sqrt{p-1}\right\rceil+12 = 2\left\lceil\sqrt{N}\right\rceil+12 & \text{for } pr \in pr^{CAT2} \end{cases} \quad (16)$$

The formula specifying the maximum correlation magnitude has been derived empirically. **Figure 6** shows the maximum correlation for both categories.

Next, **Table 2** characterizes a large number of known PRN code families in terms of their code length and the size of the resulting family as well as the maximum correlation magnitudes. The last two rows relate to the New PRN Code Family as defined by equation (7). A comparison with the existing PRN code families shows that:

- Only families #7, 10, and 11 allow for even code length, but with significant higher restrictions than for the categories of New Code Families #13 and 14. For a further discussion of this point, see also the article by J. Rushanan (2007) listed in Additional Resources.
- The maximum correlation magnitude of the New Code Family is identical to #2, 4, 7, 9, and 11.

The evaluation of PRN code families regarding their auto- and cross-correlation performance is provided next in the form of correlation histograms. **Figure 7** provides a sample histogram that also includes a listing of correlation percentiles.

The number of cross-correlation magnitudes resulting from an entire code family consisting of K sequences, each of length N, sums up to $(K^2/2 - K/2)N$, and all these correlation values form the test statistics to derive the percentiles represented in Figure 7.

The blue crosses in Figure 7 indicate the maximum/minimum relative frequency with which the corresponding correlation magnitude shows up in a specific correlation function, depending on the selection of two PRN sequences out of the full code family. If a minimum is not indicated, at least one code pair combination exists that does not adopt the corresponding correlation magnitude. The black circles indicate the mean value with which the corresponding correlation magnitude is adapted. Here the average is taken over all $K^2/2 - K/2$ potential code pair combinations.

The dashed red line in Figure 7 further indicates the cumulative frequency of the various mean values, while the green line relates to the correlation limit that could be achieved for a set of Gold codes of appropriate length.

As outlined previously, the new code family can be constructed for any code length equal to p-1, p being a prime number. For demonstration purposes, we selected a code length of 4,092 chips. On the one hand, this complies with the code

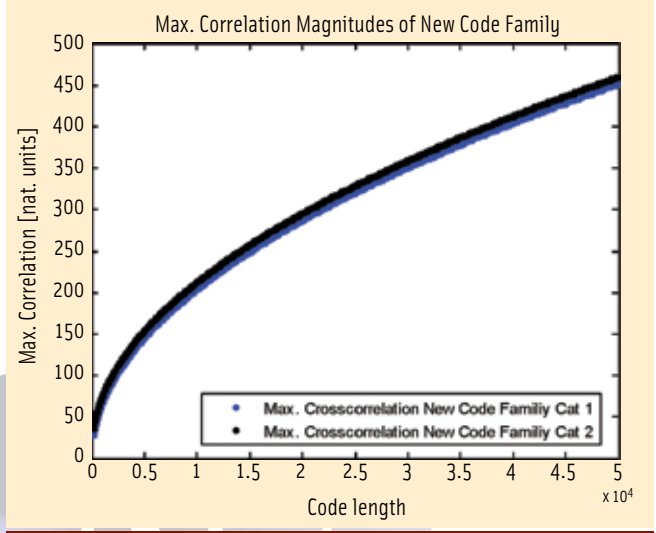

FIGURE 6 **Maximum correlation magnitudes of New Code Family**

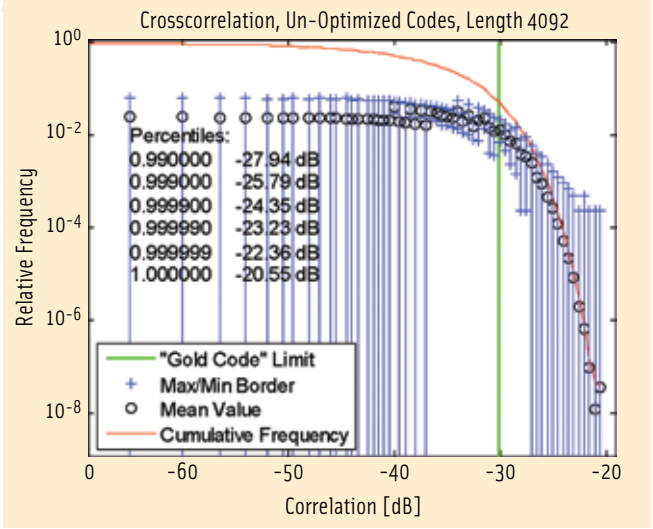

FIGURE 7 **Sample correlation histogram**

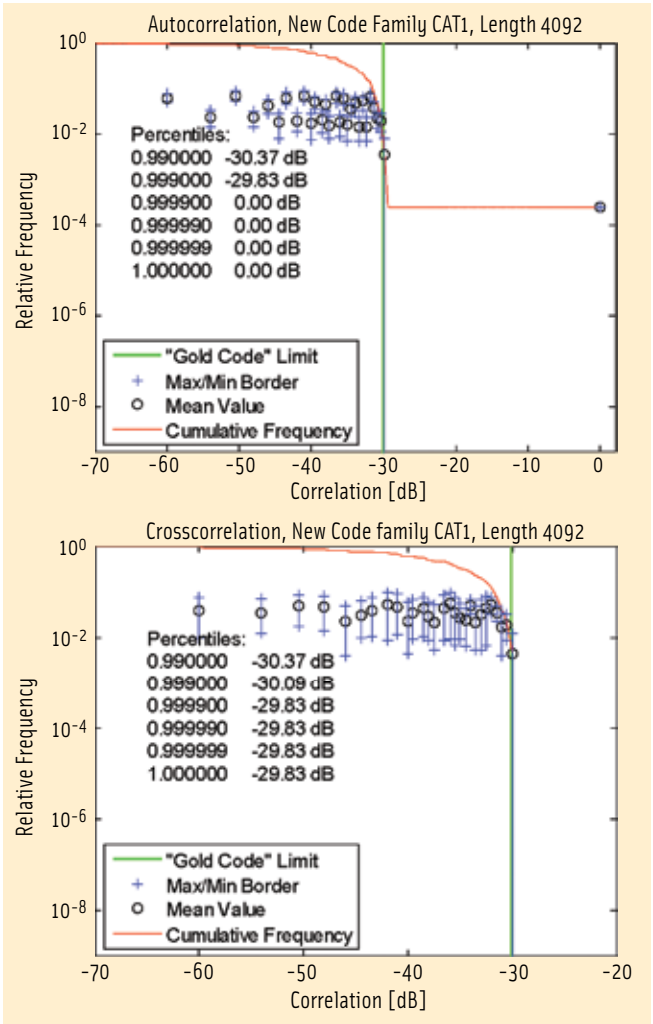

FIGURE 8 Auto- and cross-correlation histogram of New Code Family for a length of 4,092 chips

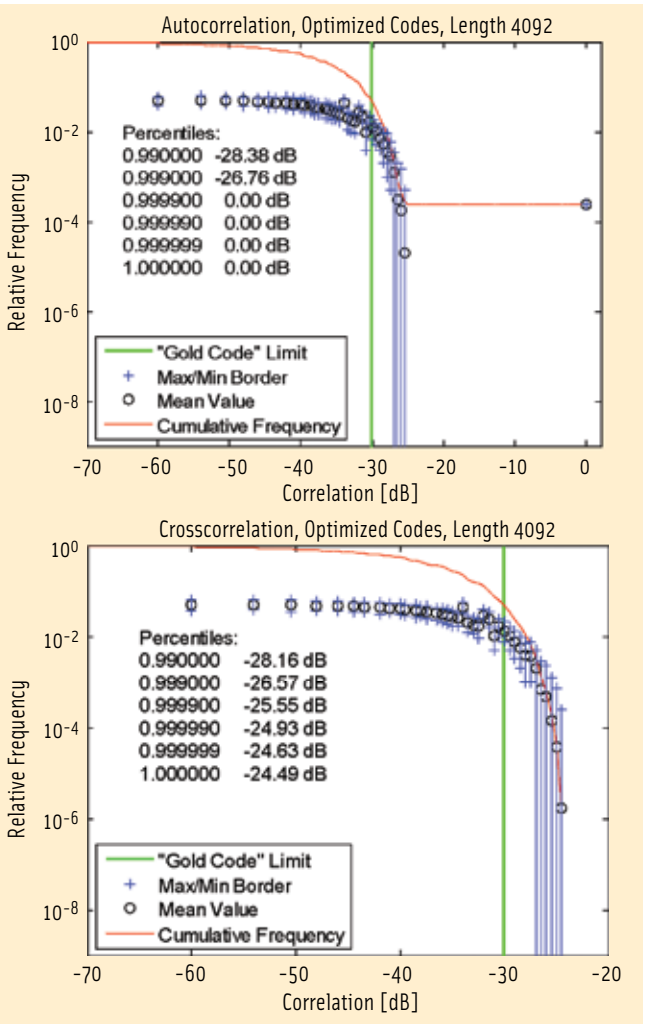

FIGURE 9 Auto- and cross-correlation histogram of optimized code family for a length of 4,092 chips

length requirement of the new code family and, on the other hand, a highly optimized code family of this length is available that we can use for comparison.

For this performance demonstration, shown in **Figures 8** and **9**, the green line needs to be seen as an indicator identifying a level of excellent correlation performance as can be obtained for Gold codes. However, please note that Gold codes of length 4,095 chips (which is very close to the code length of 4,092 that we will analyze next) do not exist because the order of the LFSR must not be a multiple of 4. The corresponding LFSR order would be 12 in this case.

The following results should only be seen as examples; similar results can be obtained for any code length with which the new code family is built. The New PRN Code Family is based on an SLCE sequence that has been derived from the primitive root element 5 according to equation (7). The selected primitive root element 5 belongs to Category 1, thus showing a slightly lower maximum correlation.

We must note that the correlation performance evaluation shown next focuses on a 0-hertz Doppler frequency offset. As has been shown on several occasions (see the article by S. Wallner *et alia*), the correlation of code families showing ideal performance at 0-hertz Doppler offset degrades when a Doppler offset is applied, converging to the performance shown by un-optimized code sets.

Figure 10 next shows the maximum absolute correlation values based on a pairwise correlation evaluation. Three different maximum correlation magnitudes were observed for a code set of length 4,092, and their relative distribution is shown in **Table 3**.

Size of Code Family. The new code family includes a number of $N/2-1$ individual codes where the code length N is given by $N=p-1$ with a prime number p.

Deriving a Subset Offering Good Odd Correlation

As already indicated at the beginning of this column, even auto- and cross-correlation are not the only measures by which to judge the performance of a PRN code family. Typically the navigation data or the secondary code bits are modulated onto the primary PRN code, applying binary phase shift keying (BPSK).

#	Name	Code Length N	Family Size	Maximum Correlation
1	Gold (odd)	2^n-1, mod(n,2)=1	$N+2$	$1+\sqrt{2(N+1)}$
2	Gold (even)	2^n-1, mod(n,4)=2	$N+2$	$1+2\sqrt{N+1}$
3	Kasami (small)	2^n-1, mod(n,2)=0	$\sqrt{N+1}$	$1+\sqrt{N+1}$
4	Kasami (large)	2^n-1, mod(n,4)=2	$(N+2)\sqrt{N+1}$	$1+2\sqrt{N+1}$
5	Bent	2^n-1, mod(n,4)=0	$\sqrt{N+1}$	$1+\sqrt{N+1}$
6	No	2^n-1, mod(n,2)=0	$\sqrt{N+1}$	$1+\sqrt{N+1}$
7	Gong	$2(2^n-1)$	$\sqrt{N}$	$3+2\sqrt{N+1}$
8	Paterson, Gong	p^2, mod(p,4)=3	$\sqrt{N}+1$	$3+2\sqrt{N+1}$
9	Paterson	p^2, mod(p,4)=3	N	$5+4\sqrt{N+1}$
10	Z4 linear, Family I	$2(2^n-1)$, mod(n,2)=1	$N/2+1$	$2+\sqrt{N+2}$
11	Z4 linear, Family II	$2(2^n-1)$, mod(n,2)=1	$(N+2)^2/4$	$2+2\sqrt{N+2}$
12	Weil	p	$(N-1)/2$	$5+2\sqrt{N}$
13	New Code Family, Category 1	p -1	$N/2$-1	$4+2\sqrt{N}$
14	New Code Family, Category 2	p -1	$N/2$-1	$12+2\sqrt{N}$

Outperforming | Excellent | Fair | Significant shortcomings

p: prime number; $n \in \mathbb{N}$

TABLE 2. Comparison of various PRN code families (Characteristics for families 1 to 12 are derived from the article, "The Spreading and Overlay Codes for the L1C Signal," by J. Rushanam.)

Correlation magnitude [natural units]	124	128	132
Correlation magnitude [dB]	-30.37	-30.10	-29.83
Relative occurrence	0.04%	75.03%	24.93%

TABLE 3. Maximum cross-correlation magnitudes and their occurrence

Whenever the navigation or secondary code bits within the integration period induce a flip of the PRN code sequence, the resulting correlation function is referred to as an *odd correlation*. The difference between the even and the odd correlation is outlined in **Figure 11**.

The odd correlation for two sequences u and v of length N is calculated according to the following formula:

$$\hat{\theta}_{u,v}(l) = \sum_{n=0}^{N-1} (-1)^{\zeta} v(n+l)u(n) \qquad (17)$$

with

$$\zeta = \begin{cases} 1 & \text{if } n \le l \\ 0 & \text{else} \end{cases}$$

Obviously, apart from even and odd correlations, a large number of additional figures of merit exist to judge the performance and compare different PRN code families. These performance measures include Excess Line Weight and Excess Welch Square Distance, as well as the correlation accounting for Doppler frequency offset.

The interested reader is invited to consult the previously referenced paper by F. Soualle to gain more insight into the different existing FOMs that can be applied for PRN code evaluation.

However, as the objective of this column is to introduce a new PRN code family, we will restrict ourselves to the even and odd correlation and ignore further evaluation of other specific properties.

We should point out that any PRN code family derived by analytical formula can only offer good *even* correlation performance. Up to now — and this also applies to the New PRN Code family introduced in this column — no PRN code family derived from closed mathematical expression is known that offers at the same time excellent even and odd correlation characteristics. The odd correlation for mathematically derived PRN code sets is generally not superior to what can be obtained from any unoptimized PRN code family.

Therefore, we need to identify ways that provide a selection of codes showing — in addition to excellent even correlation — good *odd* correlation performance. The selection of a subset of codes showing also good odd correlation performance can be accomplished by either applying a bottom-up or a top-down approach.

The bottom-up approach starts with the identification of an initial seed sequence followed by a search for sequences that keep the maximum odd correlation of the resulting set under control. The code family of GPS L1C was constructed following this concept, too.

The following discussion proposes and applies a top-down method. Due to the nature of the concept we refer to it as *iterative sifting*.

The first step is the generation of the full code family and evaluation of its performance of odd correlation. For each code

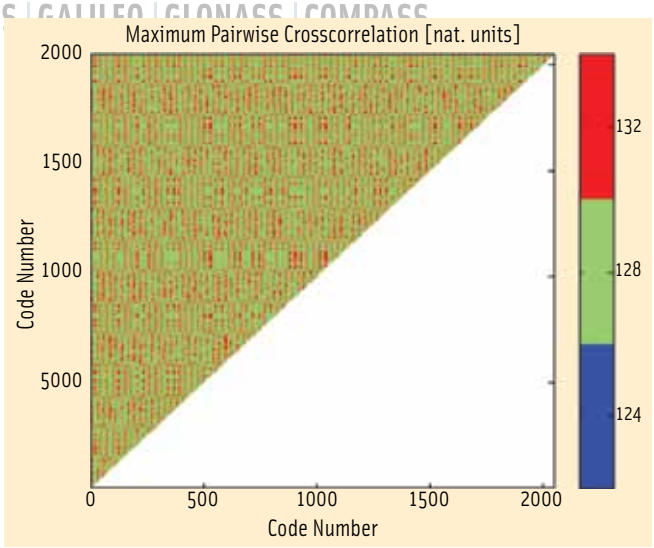

FIGURE 10 Maximum pairwise cross-correlation in nat. units

pair the maximum absolute odd correlation value is stored in matrix form, which for the New PRN Code Family results in a square matrix of size $N/2$-1.

After identifying the requirement regarding the size $\tilde{N}$ of the PRN code family to be obtained the iterative sifting process can be initialized. The concept is based on the identification of PRN codes that lead to the maximum correlation magnitude within the current set. The deletion of one of the PRN codes resulting in the maximum correlation magnitude is sufficient to produce a gain in correlation performance. In turn, this opens the door for some random optimization.

This process is continued until the code set is reduced to size $\tilde{N}$ and the result is stored. The next iteration uses the initial code family of size N and restarts the sifting process. However, due to the random nature of the process the deletion of individual PRN sequences from the overall set follows a different scheme. The two resulting code sets of size $\tilde{N}$ are compared and only the better performing one is maintained. **Figure 12** schematically outlines the overall process.

Figures 13 and **14** present the result of this selection process, using the New PRN Code family of length 4,092.

The requirement regarding the minimal size of the PRN code set was placed at 130 codes, which is considered sufficient for navigation applications. The result of the iterative sifting process is indicated in **Figure 14**, where we can see that the maximum odd correlation magnitude is reduced from 360 to 280 (in natural numbers), which corresponds to 2.2 decibels' improvement.

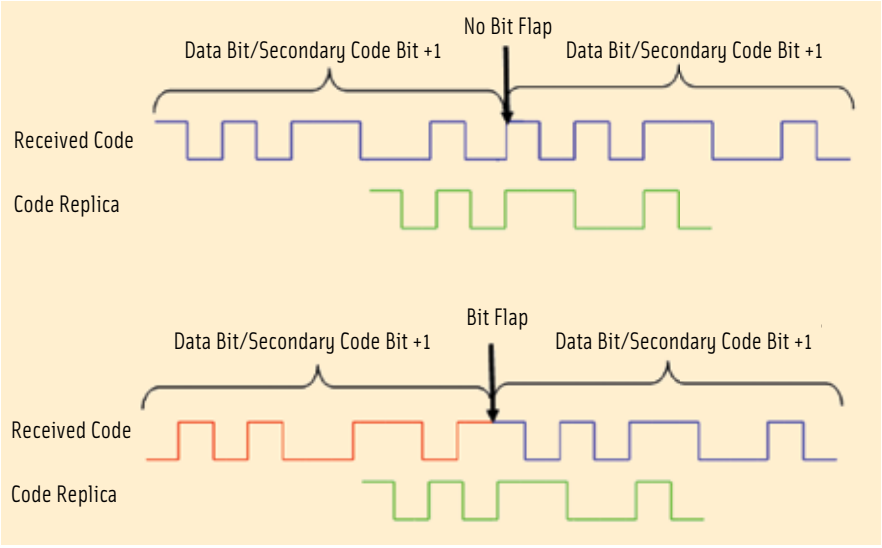

FIGURE 11 Even (top) and Odd (bottom) Correlation

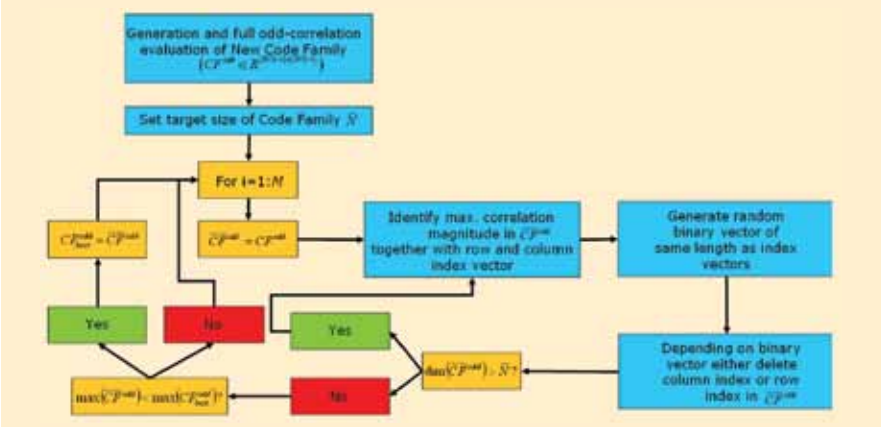

FIGURE 12 Top Down Selection Process for Odd Correlation

Conclusions

This article has presented a new family of PRN codes that can be constructed following a closed mathematical formula. This new code family offers excellent even correlation properties.

Following the approach that we have described here, PRN codes of length $N=p-1$ (p being a prime number) can be generated, allowing for a high level of fidelity regarding the code length. This produces a much higher likelihood that the code length directly matches the system requirement. Consequently, no truncation or elongation of the PRN code — which is associated with a loss of correlation performance — is required. Moreover, just one original SLCE sequence of length N is sufficient to derive a full set of $N/2$-1 PRN codes by binary-shift-and-add logic. This alleviates the need to store each chip of the PRN code in memory within the receiver device.

The code family described in this column is large enough to serve any needs in the field of navigation, be it for satellites, pseudolites, or both. A request has been initiated for a patent application on the New PRN Code Family.

Additional Resources

[1] Burton, D. M., *Elementary Number Theory,* 4th Edition, William C. Brown Publishers, 1989

[2] Gao, G. X.,.and A. Chen, S. Lo, D. De Lorenzo, T. Walter, and P. Enge, "Compass-M1 Broadcast Codes in E2, E5b and E6 Frequency Bands," *IEEE Journal of Selected Topics in Signal Processing, Special Issue on Advanced Signal Processing for GNSS and Robust Navigation,* August, 2009

[3] Gold, R., "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Transactions on Information Theory,* Vol. 13, pp. 619–621, October 1967

[4] Gong, G., "New Designs for Signal Sets with Low Cross-correlation, Balance Property and Large Linear Span: GF(p) Case," *IEEE Transactions on Information Theory,* Vol. 48, pp. 2847–2867, 2002

[5] Hadef, M.,.and J. Reiss and X. Chen, "Chaotic Spreading Codes and Their Generation," *Patent Application Publication, US 2010/0054225 A1,* March, 2010

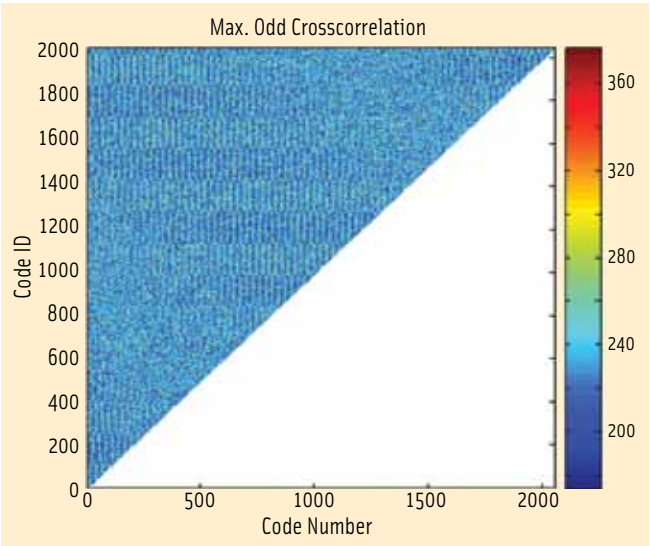

FIGURE 13 Maximum Odd cross-correlation for full set (natural units)

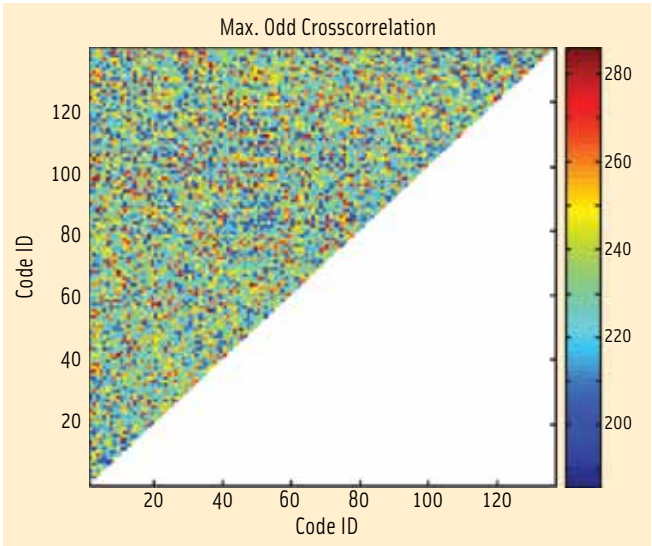

FIGURE 14 Maximum Odd cross-correlation after iterative sifting (natural units)

[5] Hein, G.W., and J.-A. Ávila-Rodríguez and S. Wallner, "The Galileo Codes and Others," *Inside GNSS,* Volume 1, September, 2006

[6] Holmes, J. K., *Spread Spectrum Systems for GNSS and Wireless Communications,* Artech House, Boston, 2007

[7] Kasami, T., *Weight Distribution Formula for some Class of Cyclic Codes*, Coordinated Science Laboratory, University of Illinois, April 1966

[8] Lempel, A., and M. Cohn and W. L. Eastman, "A Class of Balanced Binary Sequences with Optimal Autocorrelation Properties," *IEEE Transactions on Information Theory,* Vol. 23, No. 1, pp. 38–42, January 1977

[9] No, J. S., and V. Kumar, "A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span," *IEEE Transactions on Information Theory,* Vol. 35, pp. 371–379, March 1989

[10] Olsen, J. D., and R. A. Scholtz and L. R. Welch, "Bent-Function Sequences," *IEEE Transactions on Information Theory,* Vol. 28, pp. 858-864, 1982

[11] Paterson, K.G., "Binary Sequences with Favourable Correlations from Different Sets and MDS Codes," *IEEE Transactions on Information Theory,* Vol. 44, pp. 172–180, 1998

[12] Rushanan, J. (2006), "Weil Sequences: A Family of Binary Sequences with Good Correlation Properties," *IEEE International Symposium on Information Theory,* Seattle, Washington, July, 2006

[13] Rushanan, J. (2007), "The Spreading and Overlay Codes for the L1C Signal," *Journal of Navigation,* Vol. 54, No. 1, pp 43-51, 2007

[14] Sidelnikov, V. M., "Some k-valued pseudo-random sequences and nearly equidistant codes," Problems of Information Transmission, Vol.5, 1969, pp. 12–16

[15] Soualle, F., and M. Soellner, S. Wallner, et al., "Spreading Code Selection Criteria for the Future GNSS Galileo," *Proceedings of ENC 2005,* Munich, Germany, July 19–22, 2005

[16] Wallner, S., and J. J. Rushanan, J.-A., Ávila-Rodríguez, and G. W. Hein, "Galileo E1 OS and GPS L1C Pseudo Random Noise Codes—Requirements, Generation, Optimization and Comparison," *Proceedings of ION GNSS 2007,* Fort Worth, Texas, USA, September 25–28, 2007

[17] Welch, L.R., "Lower Bounds on the Maximum Cross Correlation of Signals," *IEEE Transactions on Information Theory,* Vol. 20, pp. 397–399, May 1974

[18] Winkel, J., "Spreading Codes for a Satellite Navigation System," *Patent Application Publication, US 2008/0246655 A1,* October, 2008

Author

Stefan Wallner studied at the Technical University of Munich and graduated with a Diploma in techno-mathematics. He was research associate at the Institute of Geodesy and Navigation at the Federal Armed Forces Germany in Munich from 2003 to 2010. Since 2010 he has been working as a GNSS system analysis engineer at the European Space Agency/ESTEC in Noordwijk, The Netherlands, in the field of Galileo evolution, GNSS standardization, RNSS compatibility, and future integrity provision schemes. His main topics of interests include GNSS spreading codes, the signal structure of Galileo, RF compatibility of GNSS, and advanced receiver autonomous integrity monitoring (ARAIM) concepts.

José-Ángel Ávila-Rodríguez has been since March 2010 the GNSS signal and receiver engineer of the Galileo Evolution Team at ESA/ESTEC. Between 2003 and 2010 he was research associate at the Institute of Geodesy and Navigation at the University of the Federal Armed Forces Munich. He was awarded the Bradford Parkinson prize in 2008 and the following year he received the Early Achievement Award, both from the U.S. Institute of Navigation.

Guenter W. Hein serves as the editor of the Working Papers column. He is head of the Galileo Operations and Evolution Department of the European Space Agency. Previously, he was a full professor and director of the Institute of Geodesy and Navigation at the University FAF Munich. In 2002 he received the prestigious Johannes Kepler Award from the U.S. Institute of Navigation (ION) for "sustained and significant contributions to satellite navigation." He is one of the CBOC inventors. IG