# IEEE P802.11
# Wireless LANs

## Algorithmically Derived Hop Sequences

**Date:** September 13, 1999

**Author:** Darwin Engwer, Johnny Zweig
Nortel Networks
4401 Great America Pkwy, Santa Clara, CA 95054
Phone: 408-495-7099
Fax: 408-495-8744
e-Mail: dengwer@nortelnetworks.com

## Abstract

As 802.11 evolves, the need to create additional hop sequences arises. New hop sequences are needed for use in new regulatory domains as those domains are added. This has the potential to become unwieldy and difficult to manage as the number of domains grows because the current hop sequences are each based on a precomputed base pattern that must be published as part of the standard. Products already deployed in the field will be unable to operate in these new domains because they have no knowledge of the new sequences or even the portion of the band used by the new domain (granted, some flash upgradeable products may be field upgradeable).

This paper describes a method for algorithmically computing hop sequences that have very good auto- and cross-correlation properties, summarizing work done by Edward Titlebaum. These algorithmically derived hop sequences are contrasted with the existing 802.11 hop sequences. In addition, the base method (HCC) is extended (EHCC) to provide better coverage across the band used by 802.11.

Finally, a method for incorporating these algorithmic hop sequence computation methods into the 802.11 standard is suggested.

## Introduction

Given a space of N channels, there exist N! permutations of traversing those channels. Each permutation is called a hop sequence. Some hop sequences are better than others. Hop sequences can be rated by comparing them against time or frequency shifted versions of themselves and/ or against other hop sequences. For example, a set (family) of hop sequences that possesses good auto- and cross-correlation properties is better than a family that does not[5,6].

Edward L. Titlebaum has done much work in the area:

- developing methods for transcribing hop sequences for analysis (placement-operator graphs)[1],
- formalizing the process by which hop sequences are compared and rated (hit matrices)[2,3],
- developing algorithms for cubic congruence codes (CCC)[1],
- developing the nearly ideal hyperbolic congruence codes (HCC)[4], and
- analyzing the available code generation algorithms (place-operator function comparisons)[5,6].

Titlebaum's 1992 paper[4] represents a pivotal work in the development of good families of hop sequences. The algorithm described in that paper presents the method of computing Hyperbolic Congruence Codes[1] (HCC), which are shown to be "the best compromise between auto- and cross- properties [tradeoffs]"[4,5,6].

Note that 802.11-1997 really has only one hop sequence[8] which is frequency shifted across the band. The Titlebaum HCC algorithm generates N different hop sequences[4]. Each individual HCC hop sequence has good auto-correlation properties and the code family as a whole has good cross-correlation properties.

[1] Titlebaum refers to hop sequences as "codes". The set of all codes (for a given algorithm) is called the "code family".

## Hyperbolic Congruence Codes (HCC)

The HCC hop sequences are derived from a simple formula that uses field operations on the group[2]. For full details of the Hyperbolic Congruence Codes (HCC) placement operator function, please see the reference[4]. In summary, the placement operator function is:

$$y_{HCC}(k;a) = (a / k) \bmod N \qquad k, a \in J'_N$$

Where the coefficient, a, is the family index, and k is in the group $J'_N$. k does not take the value zero. The value 1/k is the multiplicative inverse[3] of k on the field $J_N$.

As an example, consider a code family that supports 10 channels, i.e. has a code length of 10. The prime radix (N value) for such a family is 11. The code family[4] generated by the HCC algorithm is shown below in Table 1.

| SEQ \ INDEX (k) ----> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |
| 2 | 2 | 1 | 8 | 6 | 7 | 4 | 5 | 3 | 10 | 9 |
| 3 | 3 | 7 | 1 | 9 | 5 | 6 | 2 | 10 | 4 | 8 |
| 4 | 4 | 2 | 5 | 1 | 3 | 8 | 10 | 6 | 9 | 7 |
| 5 | 5 | 8 | 9 | 4 | 1 | 10 | 7 | 2 | 3 | 6 |
| 6 | 6 | 3 | 2 | 7 | 10 | 1 | 4 | 9 | 8 | 5 |
| 7 | 7 | 9 | 6 | 10 | 8 | 3 | 1 | 5 | 2 | 4 |
| 8 | 8 | 4 | 10 | 2 | 6 | 5 | 9 | 1 | 7 | 3 |
| 9 | 9 | 10 | 3 | 5 | 4 | 7 | 6 | 8 | 1 | 2 |
| 10 | 10 | 5 | 7 | 8 | 2 | 9 | 3 | 4 | 6 | 1 |

*Table 1: HCC Code Family – N=11; Family Indices (SEQ) 1 thru 10*

The HCC placement operator function is simple and fast to compute. For the mathematically inclined, the algorithm is reversible; if given the current channel and channel index, one can compute the family index.

[2] The term "group" here refers to the formal mathematical definition. That is, a field refers to a finite field, in this case the finite field $J_N$, where N is a prime number (the set of integers from 0 through N). The HCC code families are defined on the integer set $J'_N = J_N - \{0\}$, i.e. the set $J_N$ less the element '0', which is called the group $J'_N$.

[3] Mathematically, multiplicative inverses on a field can be calculated as $1 / k = k^{-1} = k^{N-2}$. Other methods that are more efficient also exist.

[4] The individual codes (hop sequences) are read from this table as horizontal rows. So, the code for family index 1 = {1, 6, 4, 3, 9, 2, 8, 7, 5, 10}.

## 802.11 Hop Sequences vs. Hyperbolic Congruence Codes (HCC)

The 802.11-1997 hop sequences are derived from a single random number sequence. The code family is generated by frequency shifting this single sequence across the band, wrapping around channel values when necessary. The net effect is similar to a Linear Congruence Code[6]. Figure 1 (below) shows the 802.11 hop sequence called Pattern 0.

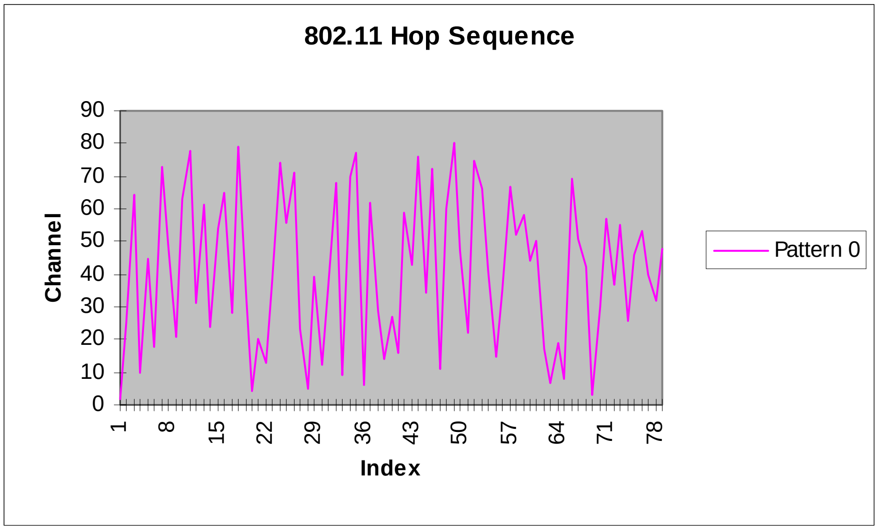


*Figure 1: 802.11 Hop Sequence – Pattern 0*

Titlebaum's HHC hop sequences are derived from a simple formula that uses field operations on the group. The HCC algorithm generates N different hop sequences[4]. Each individual HCC hop sequence has good auto-correlation properties and the code family as a whole has good cross-correlation properties. Figure 2 (below) shows the HCC hop sequence called N=79, a=1 (code length=78, family index=1).

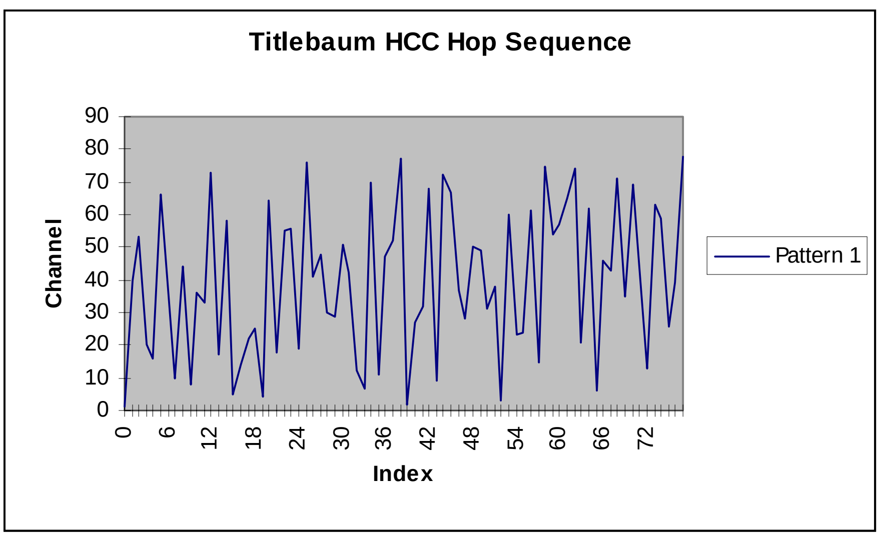


*Figure 2: HCC Hop Sequence – N=79, Family Index (SEQ) =1*

When viewing only a single hop sequence, the 802.11 and HCC hop sequences look quite similar. Now let's broaden the scope of the comparison a little and look at two hop sequences from each family. Figure 3 (below) shows 802.11 hop sequences Pattern 0 and Pattern 1.

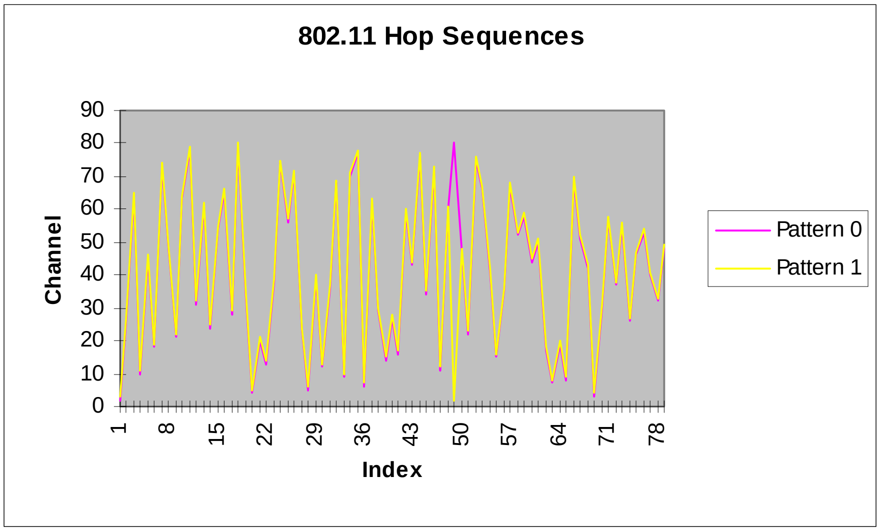


*Figure 3: 802.11 Hop Sequences – Pattern 0 and Pattern 1*

Notice that there appears to be only a single pattern graphed. There actually are two lines, but they are so close to each other they appear as a single, thick line on the graph. This is because 802.11 Pattern 0 and Pattern 1 differ only in that Pattern 1 is shifted up one frequency channel. Hence, the only noticeable difference is at index value 48, where the value for Pattern 1 wraps around to channel 2. The entire family of 802.11 hop sequences is generated in the same manner, by shifting the single hop sequence up, proceeding across the band. This, in part, leads to the 802.11 recommendation to use (in close physical proximity to each other) hop sequences from each of the 3 sets defined by 802.11; it at least separates the hop sequences by a channel delta value of 3. (Note that this is the worst-case cross-correlation between the two patterns, where they are exaclty in phase.)

In contrast, each HCC generated hop sequence is unique, yet retains the desired pseudo-random characteristics. Figure 4 (below) shows the HCC hop sequences called N=79, a=1 and a=2 (code length=78, family indexes=1 and 2).

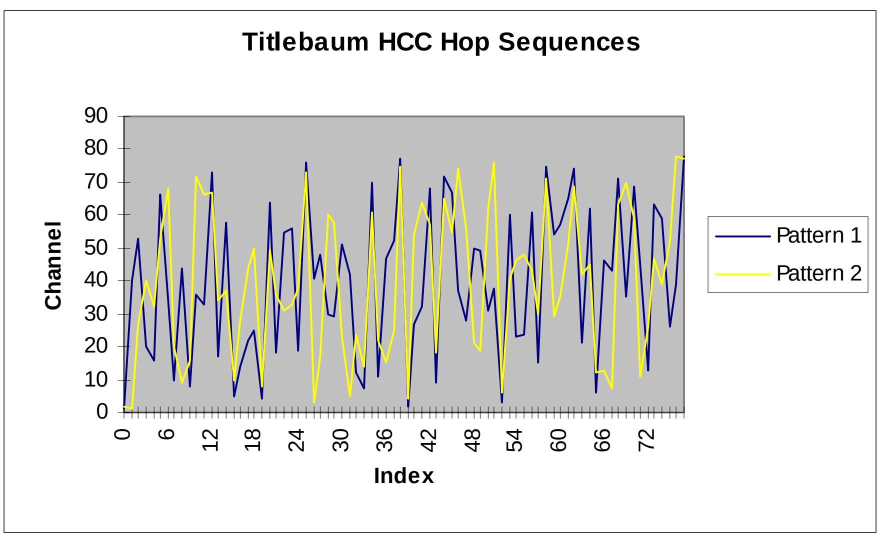


*Figure 4: HCC Hop Sequences – N=79; Family Index (SEQ) =1 and 2*

Notice that the two HCC hop sequences are quite different. Each sequence in the family is completely different from the others (and therefore has low cross-correlation with them), yet is quite easily generated from the base formula.

## Enhanced Hyperbolic Congruence Codes (EHCC)

The HCC placement operator function is based on a prime-radix. “Exactly p-1 codes of length p-1 exist for every prime, p.”[4] Hence, Titlebaum’s HCC algorithm is restricted to groups (code lengths) of size prime-1. Thus, the following code lengths are supported: 1, 2, 4, 6, 10, 12, 16, 18, 22, 28, 30, 36, 40, 42, 46, 52, 58, 60, 66, 70, 72 and 78. Coverage across the band is 22 / 79, or 28%.

The Enhanced Hyperbolic Congruence Codes (EHCC) algorithm extends the original HCC algorithm to support a larger subset of possible code lengths. The EHCC algorithm works through a process known as “deletion of the diagonals”. Consider a code family that supports 10 channels, i.e. has a code length of 10. The prime radix (N value) for such a family is 11. The code family[5] generated by the HCC algorithm is shown below in Table 2.

| SEQ \ INDEX (k) ----> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |
| 2 | 2 | 1 | 8 | 6 | 7 | 4 | 5 | 3 | 10 | 9 |
| 3 | 3 | 7 | 1 | 9 | 5 | 6 | 2 | 10 | 4 | 8 |
| 4 | 4 | 2 | 5 | 1 | 3 | 8 | 10 | 6 | 9 | 7 |
| 5 | 5 | 8 | 9 | 4 | 1 | 10 | 7 | 2 | 3 | 6 |
| 6 | 6 | 3 | 2 | 7 | 10 | 1 | 4 | 9 | 8 | 5 |
| 7 | 7 | 9 | 6 | 10 | 8 | 3 | 1 | 5 | 2 | 4 |
| 8 | 8 | 4 | 10 | 2 | 6 | 5 | 9 | 1 | 7 | 3 |
| 9 | 9 | 10 | 3 | 5 | 4 | 7 | 6 | 8 | 1 | 2 |
| 10 | 10 | 5 | 7 | 8 | 2 | 9 | 3 | 4 | 6 | 1 |

*Table 2: HCC Code Family – N=11; Family Indices (SEQ) 1 thru 10*

By the HCC algorithm, a family of codes cannot be generated for code lengths of 9 or 8, since neither 9 or 8 is equal to a prime number minus one. However, notice that the diagonals of the array in Table 1 represent the end points of the group. Thus, code families for code lengths 9 and 8 can be easily generated from the table simply by removing the diagonals. Table 3 shows such a code family with a code length of 9 (constructed by removing the diagonal of 10’s).

| SEQ \ INDEX (k) ----> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 |
| 2 | 2 | 1 | 8 | 6 | 7 | 4 | 5 | 3 | 9 |
| 3 | 3 | 7 | 1 | 9 | 5 | 6 | 2 | 4 | 8 |
| 4 | 4 | 2 | 5 | 1 | 3 | 8 | 6 | 9 | 7 |
| 5 | 5 | 8 | 9 | 4 | 1 | 7 | 2 | 3 | 6 |
| 6 | 6 | 3 | 2 | 7 | 1 | 4 | 9 | 8 | 5 |
| 7 | 7 | 9 | 6 | 8 | 3 | 1 | 5 | 2 | 4 |
| 8 | 8 | 4 | 2 | 6 | 5 | 9 | 1 | 7 | 3 |
| 9 | 9 | 3 | 5 | 4 | 7 | 6 | 8 | 1 | 2 |

*Table 3: HCC Code Family – Code Length=9, N=11; Family Indices (SEQ) 1 thru 9*

[5] The individual codes (hop sequences) are read from this table as horizontal rows. So, the code for family index 1 = {1, 6, 4, 3, 9, 2, 8, 7, 5, 10}.

Table 3 now contains a diagonal (upper left to lower right) consisting entirely of 1's. This is a necessary mathematical property of the result of removing the initial diagonal of (p-1)'s, and will be exhibited for any prime p.

Extending the process, Table 4 shows a code family with a code length of 8 (constructed from Table 3 by removing the opposite diagonal of 1's, and subtracting 1 from each value in the remaining array).

```
     INDEX (k) ---->
     1  2  3  4  5  6  7  8
SEQ-----------------------
 1 | 5  3  2  8  1  7  6  4
 2 | 1  7  5  6  3  4  2  8
 3 | 2  6  8  4  5  1  3  7
 4 | 3  1  4  2  7  5  8  6
 5 | 4  7  8  3  6  1  2  5
 6 | 5  2  1  6  3  8  7  4
 7 | 6  8  5  7  2  4  1  3
 8 | 7  3  1  5  4  8  6  2
```

*Table 4: HCC Code Family – Code Length=8, N=11; Family Indices (SEQ) 1 thru 8*

Thus, the Enhanced HCC algorithm (EHCC)[7] supports code lengths of prime-1, prime-2 and prime-3, which extends the supported code lengths to: 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 21, 22, 26, 27, 28, 29, 30, 34, 35, 36, 38, 39, 40, 41, 42, 44, 45, 46, 50, 51, 52, 56, 57, 58, 59, 60, 64, 65, 66, 68, 69, 70, 71, 72, 76, 77 and 78.  Coverage across the band is 54 / 79, or 68%.

The following code lengths **cannot** be constructed using the EHCC algorithm: 7, 13, 19, 23, 24, 25, 31, 32, 33, 37, 43, 47, 48, 49, 53, 54, 55, 61, 62, 63, 67, 73, 74, 75, 79.

## Objections to HHC

One objection to the use of HHC is that the number of "small hops" is not fixed *a priori* at a small number. That is, there are certain indices (k) for each sequence such that the channel for a given index is very close to the channel for the successive index. In the presence of narrowband interference, the objection states that both of these two successive hops may be jammed, resulting in a longer than optimal time before the system hops to a channel that is not being interfered-with.

While there is certainly merit to this objection, the weight it should be given is a function of one's conceptual model of interference in the 2.4 GHz spectrum. Those who believe that narrowband (but not actual CW) interference will dominate in the spectrum will be more concerned about the inability of the 802.11 committee to "hand pick" pseudo-random sequences with few small hops than those who think interference is most likely to come from wideband sources. Note that one of the predicted sources of such narrowband interference is BlueTooth, which has the property that the interference-source itself tends to hop away to a different (and unlikely-to-be-interfering) channel in the very near future.

It is also important to keep in mind that, even as the 2.4 GHz spectrum becomes more crowded, most users of 802.11 systems are in a position to control their environment by restricting deployment of devices that do not work well together. That is, by judiciously deploying microwave lights and ovens, DSSS and HR/DSSS 802.11 systems, BlueTooth and HomeRF systems, and 2.4 GHz cordless telephones, system administrators can typically remove the sources of interference that some designers of hop-sequence selection algorithms are worried about.

## Automatic Hop Sequence Acquisition

One large advantage of an algorithmic hop sequence generation algorithm is that systems that implement the algorithm could conceivably use hop sequences that were not defined when the implementation was built. This provides a tantalizing possibility: the "World-Ready 802.11 FH station".

The World-Ready FH station would, upon receiving a Beacon or Probe Response from an Access Point that contained a (to-be-defined) new FH Parameter Set element, be able to calculate the hop sequence for that AP and adopt it, irrespective of what regulatory domain is in operation. The Access Point would, of course, need to be properly configured with hopping parameters suitable to the local regulatory domain. But, once the APs are so configured, the mobile stations would adopt the hopping sequences and operate in an appropriate fashion for the local regulatory domain. Assuming that regulatory officials could be convinced that proper operation would be automatically enforced, we envision the possibility of an FH mobile station that could be taken anywhere in the world and operate with the local 802.11 infrastructure in accordance with local regulations.

Furthermore, implementors of 802.11 systems could define new hop-sequences more or less arbitrarily, as long as they are in accord with regulatory requirements at the destination location. This would allow producing equipment for almost any conceivable marketplace, and would relieve the 802.11 committee of the need to standardize and promulgate the hop sequences for each new regulatory domain. As long as an implementor defines a hop-sequence that obtains approval by local regulatory authorities, they could expect interoperability with equipment from other World-Ready FH vendors. By reducing the problem of defining new hop-sequences to that of picking the range of channels and defining a few parameters, 802.11 could solve the problem of defining new hop sequences once and for all.

## Summary

A method for algorithmically generating good (nearly ideal) hop sequences has been shown. Hop sequences can be simply and easily computed using the HCC formula and extended using the EHCC method, which yields 68% coverage across the band used by 802.11.

Using those methods, hop sequences need not be precomputed and conveyed via documents. Instead hop sequences can be defined and computed on the fly, as needed. A completely new set (family) of hop sequences can be defined simply by specifying the prime radix, the number of channels and the channel offset (within the band).

Those three values could be specified in a new Information Element (IE) added to the beacon. Hence, an Access Point configured for a new regulatory domain could advertise the portion of the band used by the domain and the parameters for computing the hop sequences used in that sub-band. Such an implementation would be immediately compatible with all mobile stations that understand the new IE. Additionally, a mobile station could then be moved from regulatory domain-to-domain and it would operate legally in all those environments.

References:

[1] S.V. Maric and E.L. Titlebaum, "Frequency Hop Multiple Access Codes Based Upon the Theory of Cubic Congruences", IEEE Transaction on Aerospace and Electronic Systems, November 1990

[2] Bellegarda, J.R. and Titlebaum E.L., "The Hit Array: An Analysis Formalism for Multiple Access Frequency Hop Coding", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 27, No. 1, January 1991, pp. 30-39.

[3] Bellegarda, J.R. and Titlebaum E.L., "The Hit Array: A Synthesis Tool for Multiple Access Frequency Hop Signals", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 29, No. 3, July 1993, pp. 624-635.

[4] S.V. Maric and E.L. Titlebaum, "A Class of Frequency Hop Codes with Nearly Ideal Characteristics for Use in Multiple-Access Spread-Spectrum Communications and Radar and Sonar Systems", *IEEE Transactions on Communications*, Vol. 40, No. 9, September 1992, pp. 1442-1447

[5] Z. Kostic and E.L. Titlebaum, "The Design and Performance Analysis for Several New Classes for Optical Synchronous CDMA and for Arbitrary-Medium Time-Hopping Synchronous CDMA Communication Systems", *IEEE Transactions on Communications*, Vol. 42, No. 8, August 1994

[6] E.L. Titlebaum, "Frequency- and Time-Hop Coded Signals for use in Radar and Sonar Systems and Multiple Access Communication Systems", self-published, a summary of all the various methods of computing hop sequences, including a comparison of the relative strengths and weaknesses of each method.

[7] Clements, Ken, "Enhanced Hyperbolic Congruence Codes (EHCC) with Improved Group Coverage for Multiple Access Communications Systems", Netwave internal engineering document, circa Aug 1995. This document describes the extension of the group coverage of the HCC algorithm from prime-1 to prime-1, prime-2 and prime-3 by deletion of the diagonals, substantially increasing the coverage space for the algorithm. (22 / 79 → 54 / 79, which represents a coverage improvement from 28% → 68% in the band used by 802.11).

[8] IEEE 802.11-1997 Standard: Clauses 14.6.3 - 14.6.8 FH hop sequence specs; Clause 14.8.2.1.2 FH regulatory domain codes; Annex B Hopping Sequences.