Spread Spectrum Primer

What is spread spectrum, anyway?

by Randy Roberts KC6YJY (ex-WA6BFN)

Spread spectrum uses wideband, noise-like signals. Because spread spectrum signals are noise-like, they are hard to detect. Spread spectrum signals are also hard to intercept or demodulate. Further, spread spectrum signals are harder to jam (interfere with) than narrowband signals. These low detectability and anti-jam features are why the military has used spread spectrum for so many years. Spread signals are intentionally made to be much wider-band than the information they are carrying to make them more noise-like.

Spread spectrum signals use fast codes that run many times the information bandwidth or data rate. These special "Spreading" codes are called "Pseudo Random" or "Pseudo Noise" codes.

Spread spectrum transmitters use the same transmit power levels as narrowband transmitters. Because spread spectrum signals are so wide, they transmit at a much lower watts-per-hertz power density than narrowband transmitters. This lower power density gives spread signals a big plus. Spread and narrowband signals can occupy the same band, with little or no interference. This capability is the main reason for all the interest in spread spectrum today.

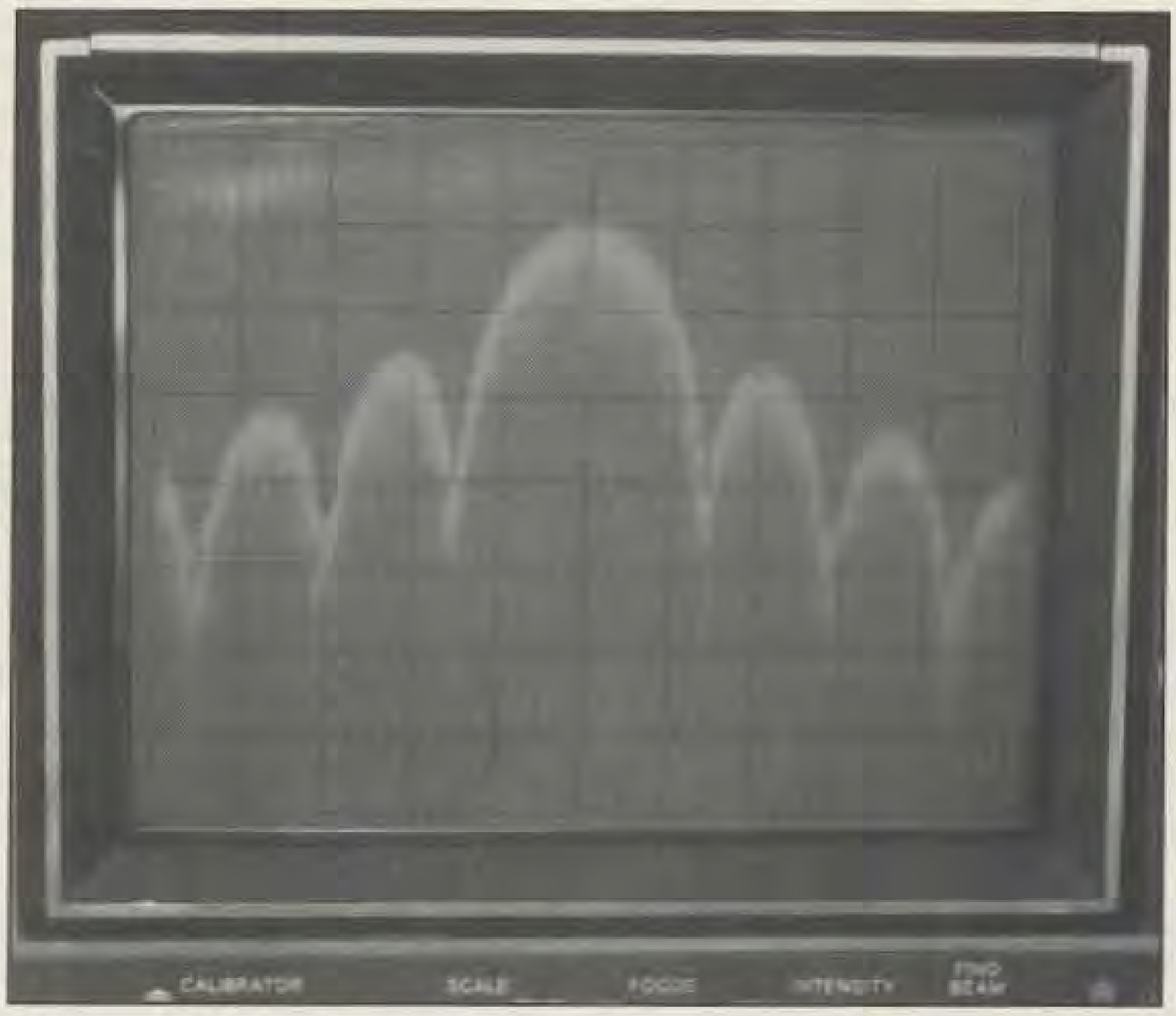

Photo A. Direct sequence spread spectrum signal (un-filtered BPSK). Note the suppressed carrier. Center freq.= 52 MHz with a 1.5 megabit/second PN (31 stage PN generator). Horiz. scale = 1 MHz/div. Vert. scale = 10 dB/div.

What's Spread Spectrum?

Spread spectrum radio communication is igniting much discussion and speculation lately. In the last few years there has been a lot of media attention, congressional interest (*IEEE Spectrum*, "Spread Spectrum Goes Commercial," August 1990, by Donald L. Schilling, Raymond L. Pickholtz and Laurence B. Milstein, pp. 40-45), FCC rulemaking, commercial product announcements and marketing hoopla about this exciting new field. Several very good articles on spread spectrum (SS) have appeared in ham radio literature and the ARRL's *Spread Spectrum Sourcebook* has been in print for several years now. With all of this activity you may still have a few questions about spread spectrum, how it applies to hams, how it works and in general what all this alphabet soup (like PCN, PCS, CDMA, TDMA and frequency hopping) is all about. See the sidebar for a definitive guide. This article is intended to gently lead you through some of the practical details of today's modern commercial (and soon to be ham) radio spread spectrum technology and help you gain a basic understanding of the principles involved in SS.

In 1983 the FCC issued a notice of proposed rule making authorizing the low power use of spread spectrum techniques on a shared frequency basis in the Industrial, Scientific and Medical (ISM) frequency bands of 900, 2400 and 5500 MHz. These bands are also shared with amateur radio operations—so we hams have a direct stake in what happens with this kind of equipment. Since 1983 the FCC has revised and clarified the rules for spread spectrum operation under Part 15 of their rules. Hams have been able to legally use spread spectrum under Part 97 rules for a number of years, also. However, the FCC rules for ham spread spectrum have been quite restrictive and have had the net effect of almost eliminating ham radio experimentation in spread spectrum techniques. Recent commercial developments with Part 15 equipment and a new FCC Special Temporary Authority (STA) (R. A. Buaas K6KGS request for STA, FCC file number 7230-A, granted April 17, 1992) provide a renewed impetus to the amateur community to make more use of spread spectrum techniques. In light of the possible awakening of a ham spread spectrum community, I hope to spur some interest in the ham builder/experimenter to put some of these ideas to practical use.

More About Spread Spectrum

Simply put, spread spectrum trades a wider transmission bandwidth for better signal-to-noise ratio and reduced transmitted power density. Two types of spread spectrum implementation are in fairly common use today: Frequency Hopped and Direct Sequence. Frequency hop (FH) and direct sequence (DS) are pretty well known, mature techniques today. Other more exotic forms of spread spectrum such as chirp, time hopping and hybrids of frequency hop and direct sequence are not in general use in low-cost Part 15 equipment and will probably remain only in the military province for several more years. The following paragraphs will describe frequency hop and direct sequence techniques in a little more detail and show that pseudo-noise code techniques provide the common thread through all spread spectrum types.

Frequency Hop

Frequency hopping can provide the easiest method of utilizing spread spectrum. Any radio with a digitally controlled frequency synthesizer can (theoretically) be converted to a frequency hopper. This conversion requires the addition of a pseudo noise code generator that is used to select the frequencies for transmission or reception. Most hopping systems utilize uniform frequency hopping over a band of frequencies. This is not absolutely necessary if both the transmitter and receiver of the system know in advance what frequencies are to be skipped. Thus, a frequency hopper in, say, 2 meters could be made that would skip over commonly used repeater input and output frequency pairs. A frequency hopped system can use analog or digital carrier modulation and can be designed using conventional narrowband radio techniques. Dehopping in the receiver is done by a synchronized PN code generator which drives the receiver's local oscillator frequency synthesizer.

Direct Sequence

The most practical, all-digital version of spread spectrum is direct sequence. A direct sequence system uses a locally generated pseudo noise code to encode digital data to be transmitted. The local code is generated at a rate of 10 to 100 times the data rate to be transmitted. Data for transmission is simply exclusive-OR'd with the faster pseudo noise code. The composite pseudo noise and data can be passed through a data scrambler to randomize the output spectrum (and thereby remove discrete spectral lines). A direct sequence modulator is then used to double sideband suppressed carrier modulate (also called Binary Phase Shift Keying—BPSK) the carrier frequency to be transmitted, resulting in a signal spectrum as shown in Photo A. Other forms of carrier modulation are possible with direct sequence, however BPSK or differential phase shift keying (DPSK) are the simplest and most often used techniques.

A spread spectrum receiver uses a locally generated replica pseudo noise code along with a receiver correlator to separate out only the desired coded information or messages from all possible signals. A spread spectrum correlator can functionally be thought of as a very special matched filter—it responds only to signals that are encoded with a pseudo noise code that matches its own locally generated replica code. Thus, a spread spectrum correlator can be "tuned" to different codes simply by changing its local code. This correlator does not respond to man-made, natural or artificial noise or interference. It responds only to spread spectrum signals with identical matched signal characteristics and encoded with the identical pseudo noise code.

Why use the wideband signals—isn't narrowband CW or packet better? The use of these special codes in spread spectrum communications makes signals appear as wideband, noise-like signals on a spectrum analyzer. It is this very characteristic that inherently makes spread spectrum signals hard to detect or demodulate. In other words, spread spectrum signals are harder to detect on narrowband equipment because the signal's energy is spread over a bandwidth of maybe 100 times the information bandwidth.

The spread of energy over a wide band of frequencies makes spread spectrum signals very unlikely to interfere with narrowband co-channel or adjacent channel communications. Narrowband communications, conversely, cause little to no interference to spread spectrum communications systems because the correlation receiver effectively integrates over a very wide bandwidth to recover a spread spectrum signal. The correlator actually then "spreads" out a narrowband interferer over the receiver's total detection bandwidth and thus only the total integrated signal density or signal-to-noise ratio determines whether there will be interference or not. All spread spectrum systems have a threshold or tolerance level of interference beyond which useful communication ceases. This tolerance level or threshold is related to the spread spectrum processing gain. Processing gain is the ratio of the radio frequency (RF) bandwidth to the information bandwidth.

Typical SS anti-jam (AJ) radios have a processing gain of from 10 to 20 dB, depending on the data rate. They can tolerate total jammer power levels of from 0 to 8 or 10 dB (jamming margin) stronger than the desired signal. Yes, the system can work at negative signal-to-noise ratios in the RF bandwidth (signals buried in the noise) because of the processing gain of the receiver's correlator.

Besides being hard to intercept and jam, spread spectrum signals are hard to exploit or spoof. One cannot get any useful information from a scanner tuned to a spread spectrum signal. Spread spectrum signals also are naturally more secure than narrowband radio communications. Thus, spread spectrum signals can be made to have any degree of message privacy that is desired—you can have all the private channels you want with spread spectrum. The very nature of spread spectrum allows military or intelligence levels of privacy and security, if desired, to be had with minimal complexity.

Frequency Re-Use and Multiple Access

Multiple spread spectrum signals on the same frequency or in the same frequency band can be accommodated through various techniques of multiple access or diversity. The nature of PN codes and correlators allow what is called CDMA (code division multiple access). Time division multiple access is also commonly used with spread spectrum. Frequency and space or polarization are also used to increase the number of users or network size of spread spectrum networks. Sometimes combinations of the above multiple access techniques are used to achieve special system characteristics.

Multiple access techniques can provide for frequency re-use, elimination or reduction of interference, increased system capacity, or to provide for "private" channels. The newest methods for digital cellular, micro-cell and worldwide LEO satellite mobile communications will use SS and CDMA or TDMA to efficiently utilize the frequency spectrum they will be allocated. Commercial voice and data PCNs and PCS's that operate over cordless telephone-like ranges of up to 5,000 feet between micro or nano cell sites will also use various SS multiple access techniques to achieve frequency re-use and spectral efficiency.

Finally and most importantly, the major benefit of spread spectrum communication is that data communications can be provided at data rates of 10 or 20 times normal wired or narrowband radio communications rates, with automatic protocols that virtually eliminate bit and message errors. Thus, digital voice, computer-to-computer, BBS, networking and other demanding communications can be provided error-free at a reasonable cost. This data reliability and integrity are the most important reasons for spread spectrum communications.

Now, the Catch

Sold on spread spectrum yet? Sounds great doesn't it? Note, however, that above I described how each type of spread spectrum worked when each receiver was presumed to have PN synchronization with its companion transmitter. This requirement for PN sync is what makes spread spectrum system design tough. There are three major problems in spread spectrum PN systems: acquisition, synchronization and tracking. All three problems are part of the general problem of estimation and/or tracking of PN code phase (timing) and frequency. These problems cause all the complexity that is associated with PN system operations. Sync problems are slightly different with each type of spread spectrum, but the main problem is the same. How does a receiver's PN generator rapidly, without significant loss of data, lock onto and track changes in a transmitter's PN code generator? A complete answer to this question is really beyond the scope of this introductory article; however, the secret lies in the design of the receiver correlator and its related processing. Current commercial Part 15 equipment uses both serial (sequential or trial and error) and parallel digital correlators. Many of these commercial designs use custom ASIC or LSI chips to accomplish the required PN acquisition and tracking operations.

Interfacing and Networking

The latest generation of commercial Part 15 SS radios, some soon to be available to hams (in a private correspondence with Mr. Dewayne Hendricks WA8DZP, president of Tetherless Access, Ltd., in February 1992, Dewayne stated that Tetherless radios will soon be available to hams through PacComm in Florida), are easily interfaced to any asynchronous communications equipment at data rates up to several hundred kB/sec. No special interface circuitry is required. The radio transmits and receives in half duplex mode—that is, it either transmits or receives data at any instant of time. The terminal hooked to the radio determines whether the radio is transmitting or receiving by setting the "Request to Send" line. Several options are available for hardware/software handshaking with the "Clear to Send" and "Device Carrier Detect" signal lines. To summarize the typical SS radio capability, the equipment can be thought of as a radio combined with a digital modem and a form of packet-radio-like TNC. Several of the commercially available SS radios (some of the more commonly available commercial SS radios are sold by GRE America, Symbol Technologies, Proxim, Senses Data Corporation, Cylink, O'Neil Communications and Qualcomm) include AX.25, X.25 or TCP/IP networking protocols software or firmware. At the current time these radios can use small networks that can be built up, entirely by software, with up to 32 or more network nodes, thus providing limited PCN/PCS capabilities. Typical SS radios in the network can be designated to be a digipeater (a store-and-forward, single-frequency repeater) by software. Several digipeaters can also be connected in tandem to extend network communications well beyond simple "line of sight" radio ranges.

Continued on page 77

Spread Spectrum Primer

Continued from page 32

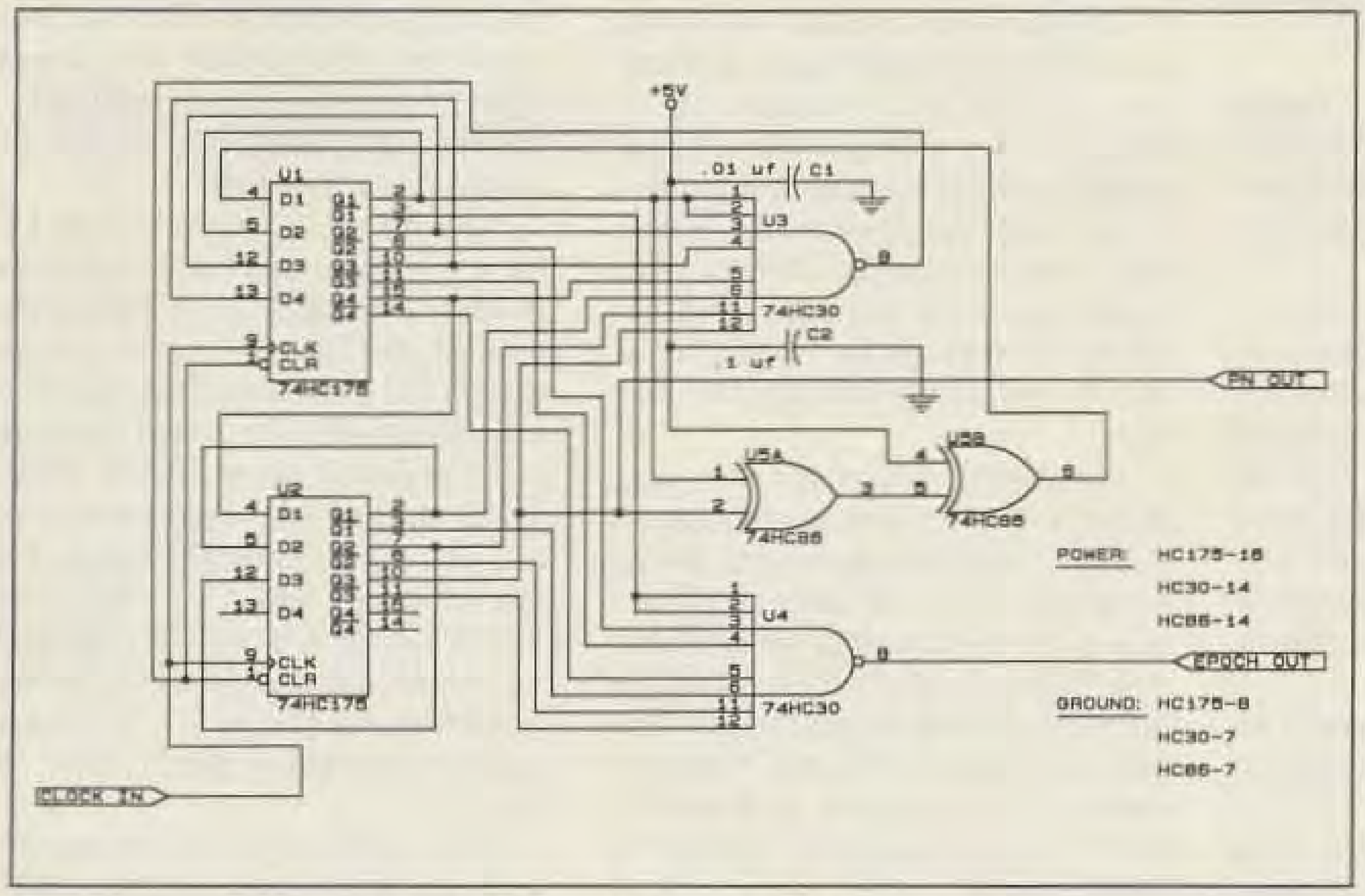

Figure 1. Simple 7-stage PN generator.

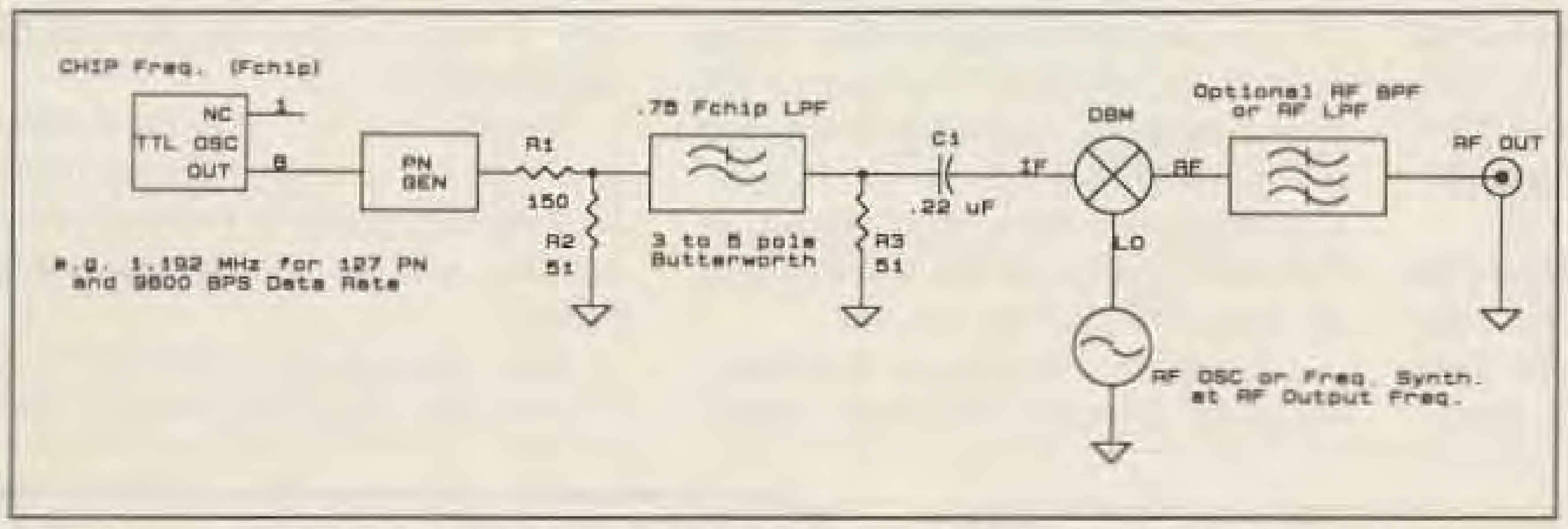
CHIP Freq. (Fchip)
NC
TTL OSC
OUT
PN GEN
R1
150
R2
51
.75 Fchip LPF
3 to 5 pole Butterworth
R3
51
C1
.22 uF
IF
DBM
RF
LO
Optional RF BPF or RF LPF
RF OUT
RF OSC or Freq. Synth. at RF Output Freq.
e.g. 1.192 MHz for 127 PN and 9600 BPS Data Rate

Figure 2. Filtered BPSK modulator block diagram.

Use of dedicated PCs or Macs with SS radios will be necessary until an integrated and well-defined data communication interface set of standards have been generated (commercial work along this line is being done by the IEEE 802.11 committee—hams haven't started this effort yet). The major feature that an industry standard hardware/software interface provides is a very simple and flexible way to channel (or multiplex) diverse sources and sinks of data to/from SSradio equipment. Standard PC or Mac (Appletalk) based multiple COM channel boards are being integrated into commercial SS radio host PCs and message routing software can be easily modified to handle multiple async data rates and protocols.

Are We Hams Ready for SS?

A very important part of a foreseeable nationwide spread spectrum system is the ability of the spread spectrum system to interface with other existing packet-based terrestrial and/or satellite-based or other amateur radio communications facilities. Several communication switching centers (or gateways) could be installed at various points throughout the US to handle digital voice, fax, teletype or other communications that require routing outside a national spread spectrum network or national ham radio PCN/PCS. Standard ham communications traffic and protocols could be transparently handled via these gateways. Will SS techniques have any impact on ham radio in the near future? Probably not—unless a renewed phase of ham radio experimentation takes place. Personal computers are now a fact of life in ham radio. So is packet. Will SS become old hat and used every day, like VHF/UHF SSB is? Time will tell. I think SS is one of the bigger challenges for hams—with ingenuity and dedication hams may enter the 21st century using SS and keeping most of our bands out of the hungry commercial interests' hands. 73

HOW TO GENERATE A LEGAL FCC PN CODE

Here is one tried and true (almost foolproof) Pseudo Noise (PN) generator circuit that requires no EPROM or PLD programmer (or software either.) The main advantage of this design is that it generates a seven-stage, length 127 maximal length shift register sequence that is legal to use under current FCC Part 97 amateur radio rules.

Simple, short length (four- to 13-stage) maximal length shift register (MLSR) sequence generators are often used to provide simple PN code generators for SS systems. These simple generators usually perform very well when started from the correct initial conditions or when reset at power up. However, most of these simple circuits can hang up and stop generating anything (they can get stuck) when an all ones (or an all zeroes) condition occurs. Which condition that causes hang up or how it got to this condition is immaterial—the darn thing is broken when this happens! The circuit concept shown in Figure 1 solves this problem very nicely and even includes an EPOCH sync detector as well (for data timing, scope sync, or whatever).

The circuit of Figure 1 is built from two 74HC175 shift registers, one 74HC86 and two 74HC30 NAND gates. As shown, the generator uses feedback from the last shift register stage as well as from the first shift register stage, as the FCC requires. This connection, when started from the all-zeroes state, will always generate the correct MLSR sequence. The top NAND gate looks for the occurrence of an all-ones condition (an indication of being stuck) and resets the shift registers to all zeroes if this condition should ever occur. The bottom NAND gate detects the occurrence of the all zeroes condition which marks the start of a PN cycle of length 127, also known as a PN EPOCH. The EPOCH signal is coincident with the start of the code repeat cycle and is useful for sampling or synchronizing input data for Direct Sequence Spread Spectrum (DSSS) modulation.

HOW TO GENERATE A USEFUL BPSK SIGNAL

Figure 2 shows a block diagram of a BPSK modulator that is useful on the ham bands. Spectrum limiting (both pre-modulation and RF bandpass filtering) is included in this design. As the unfiltered BPSK spectrum photo shows, Spread Spectrum BPSK is a relatively wideband modulation that can splatter out of a band. Pre- or post-modulation filtering must be used for most ham applications.

The clock for the PN generator, shown in Figure 1, is derived from a TTL crystal oscillator. This furnishes the "chip" clock signal. The chip clock must be 127 times the data rate for proper operation with this PN generator. The PN generator's output drives an impedance matching circuit, then a passive LC, a three- to five-pole Butterworth low-pass filter. This filter uses a cutoff frequency approximately 0.75 times the chip clock rate. This filter is used to "round" off the sharp edges and spikes that are present on the TTL output of the PN generator. This filtered, AC-coupled signal then drives the IF (DC-coupled port) of a doubly-balanced mixer (DBM). The LO port of the mixer is driven by a crystal oscillator-multiplier chain or a frequency synthesizer to provide an RF carrier for the modulator. Finally, the mixer's RF port drives a bandpass filter to provide the modulator's output RF signal. Optionally, just an output low-pass filter that reduces transmitter harmonics can be used instead of the bandpass filter. Further amplification and frequency conversion, if needed, comes at this point in an amateur radio SS transmitter.

SPREAD SPECTRUM GLOSSARY

AJ	Anti-Jam—designed to resist interference or jamming.
BPSK	Binary Phase Shift Keying—digital DSB suppressed carrier modulation.
CDMA	Code Division Multiple Access—a way to increase channel capacity.
CHIP	The time it takes to transmit a bit or single symbol of a PN code.
CODE	A digital bit stream with noise-like characteristics.
CORRELATOR	The SS receiver component that demodulates a spread spectrum signal.
DE-SPREADING	The process used by a correlator to recover narrowband information from a spread spectrum signal.
DIVERSITY	Sharing a signal characteristic to allow more users in the same frequency band.
DPSK	Differential Phase Shift Keying—a simplified BPSK where only data transitions are transmitted.
MULTIPLE ACCESS	A method for accomodating more users in the same frequency band.
NARROWBAND	A signal whose bandwidth is on the order of its information bandwidth.
NOISE-LIKE	Having properties that cause the appearance of true random noise.
PCN	Personal Communication Network.
PCS	Personal Communication System.
PN	Pseudo Noise—a digital signal with noise-like properties.