# EFFICIENT MULTIPLEX FOR BAND-LIMITED CHANNELS:
## Galois-Field Division Multiple Access

H.M. de Oliveira, R.M. Campello de Souza and A.N. Kauffman
CODEC- Grupo de Pesquisas em Comunicações
Departamento de Eletrônica e Sistemas - CTG- UFPE
C.P. 7800, 50711-970, Recife-PE, Brazil
e-mail: {hmo,ricardo}@npd.ufpe.br

**Abstract**
*A new "Efficient-bandwidth code-division-multiple-access (CDMA) for band-limited channels" is introduced which is based on finite field transforms. A multilevel code division multiplex exploits orthogonality properties of nonbinary sequences defined over a complex finite field. Galois-Fourier transforms contain some redundancy and only cyclotomic coefficients are needed to be transmitted yielding compact spectrum requirements. The primary advantage of such schemes regarding classical multiplex is their better spectral efficiency. This paper estimates the "bandwidth compactness factor" relatively to Time Division Multiple Access TDMA showing that it strongly depends on the alphabet extension. These multiplex schemes termed Galois-field Division Multiplex (GDM) are based on transforms for which there exists fast algorithms. They are also convenient from the hardware viewpoint since they can be implemented by a Digital Signal Processor.*

Keywords- Digital multiplex, Code-divison multiple access, Hartley-Galois transform, Finite field transforms, Spread sequence design.

### 1. Introduction

The main title of this paper is, apart from the term multiplex, literally identical to a Forney, Gallager and coworkers paper issued more than one decade ago [FOR et al. 84], which analyzed the benefits of coded-modulation techniques. The large success achieved by Ungerboeck's coded-modulation came from the way redundancy was introduced in the encoder [UNG 82]. In classical channel coding, redundant signals are *appended* to information symbols in a way somewhat analogous to time division multiplex TDM (envelope interleaving). It was believed that introducing error-control ability would increase bandwidth. An efficient way of introducing such an ability without sacrificing rate nor requiring more bandwidth consists in adding redundancy by an alphabet expansion. This technique is particularly suitable for channels in the narrow-band region. A similar reasoning occurs in the multiplex framework where many people nowadays believe that mux must increase bandwidth requirements.

In the present work, the coded-modulation idea is adapted to multiplex: Information streaming from users are not combined by interleaving (like TDM) but rather by a *signal alphabet expansion*. The mux of users' sources over a Galois Field GF(p) deals with an expanded signal set having symbols from an extension field $GF(p^m)$, m>1. As a consequence, the multiplex of N band limited channels of identical maximal frequency B leads to *bandwidth requirements less than* N B, in contrast with TDMed or FDMed signals.

The design of such an "efficient bandwidth mux" is based upon Galois field Transforms (GFT) such as the Finite Field Fourier Transform (FFFT) introduced by Pollard [POL 71]. The FFFT been successfully applied to perform discrete convolution and image processing [REE et al. 77, REE&TRU 79], among many other applications. In this paper we are concerned with a new finite field version [CAM et al. 98] of the integral transform introduced by R.V.L. Hartley [HAR 42, BRI 92]. Alike classical Galois-Fourier transforms [BLA 79, CAM&FAR 85], Finite Field Hartley transforms (FFHT) defined on a Gaussian integer set $GI(p^m)$ [CAM et al. 98] contains some redundancy and only the cyclotomic coset leaders of the transform coefficients need to be transmitted. This yields a new "Efficient-bandwidth Code Division multiplex for band-limited channels". These multiplexes may present lower bandwidth requirements than TDM. Tradeoffs between the extension of the alphabet and the bandwidth are exploited in the sequel. This paper shows that the "bandwidth compactness factor" relatively to TDM depends on the length m, the alphabet extension.

Another point to mention is that the superiority of digital mux regarding analog mux is essentially due to the low complexity of TDM. The majority of current multiplex systems follows plesiochronous (PDH) or synchronous (SDH) hierarchy [SIL&SHA 96]. Besides presenting higher spectral efficiency (bits/s/Hz) than classical multiplex, the new code division multiplex (CDM) schemes introduced here are based on fast transforms, so they also seem to be attractive from the implementation viewpoint [HOU 87]. Although most mux systems today intended to optical fiber which are not yet bandlimited channels, multiplex has also been adopted on satellite channels. Applications of such a multiplex will be on transponders and more probably on *cellular mobile* *communications*. Cable Television (CATV) can also benefit of such a technique.

## 2. A New Mux Scheme: Galois-Division-Multiplex

Digital multiplex normally alludes Time Division Multiplex (TDM). However, it can also be achieved by Coding Division Multiplex (CDM) which has recently been the focus of interest, specially after the IS-95 standardization of the CDMA system for cellular telephone [QUAL 92]. The CDMA is now becoming the most popular multiple access schemes for mobile communication. In this section we introduce a new class of mux schemes based upon finite-field transforms which can be implemented by fast transform algorithms. *Classical multiplex increases simultaneously the transmission rate and the bandwidth by the same factor*, keeping thus the spectral efficiency unchanged. In order to achieve (slight) better spectral efficiencies, classical CDMA uses waveforms presenting a nonzero but residual correlation. We introduce here a new and powerful issue on CDMA techniques.

Given a signal v over a finite field GF(p), we deal with the Galois domain considering the spectrum V over an extension field $GF(p^m)$ which corresponds to the Finite Field Transform (Galois Transform) of the signal v [BLA 79, CAM et al. 98].

As an alternative and attractive implementation (figure 1), the multiplex can be carried out by a Galois Field Transform (FFFT/FFHT) so the DEMUX corresponds exactly to an *Inverse Finite-Field Transform* of length $N \mid p^m-1$.

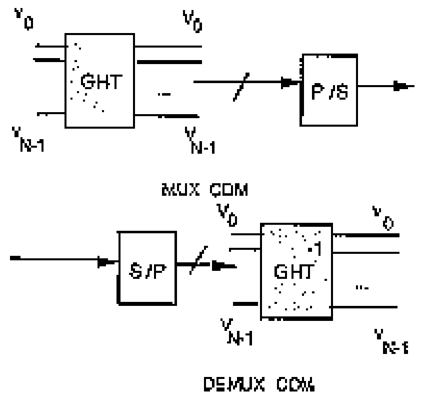
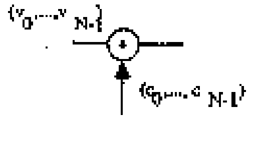



Figure 1. Implementation of Galois Field Transform (GFT) multiplex.

Each symbol in the ground field GF(p) has duration T seconds. An N-user mux can be designed on the extension field $GF(p^m)$ where $N \mid p^m-1$. For the sake of simplicity, we begin with m=1 and consider a (p-1)-channel mux as follows. Typically, we can consider GF(3) corresponding to Alternate Mark Inversion (AMI) signaling.

<u>Definition</u>. A Galois modulator carries a pairwise multiplication between a signal $(v_0, v_1, ..., v_{N-1})$, $v_i \in GF(p)$ and a carrier $(c_0, c_1, ..., c_{N-1})$, with $c_i \in GI(p)$. ■

A pictorial representation of a Galois modulator:




A (p-1)-CDM considers digital carrier sequences per channel as versions of the cas function $\{cas_i k\}_{k=0}^{p-1}$ over the Galois (complex) field GI(p). The cas (cos and sin) function is defined in terms of finite field trigonometric functions [CAM et al. 98] according to $cas_i k := \cos_i k + \sin_i k$.

**Carrier 0:**

$\{cas_0 0 \;\; cas_0 1 \;\; cas_0 2 \;\; ... \;\; cas_0 (N-1)\}$

**Carrier 1:**

$\{cas_1 0 \;\; cas_1 1 \;\; cas_1 2 \;\; ... \;\; cas_1 (N-1)\}$

...

Carrier j:

$\{cas_j 0 \;\; cas_j 1 \;\; cas_j 2 \;\; ... \;\; cas_j (N-1)\}$

...

**Carrier N-1:**

$\{cas_{N-1} 0 \;\; cas_{N-1} 1 \;\; cas_{N-1} 2 ... cas_{N-1} (N-1)\}$.

The cyclic digital carrier has the same duration T of an input modulation symbol, so that it carries N slots per data symbol. The interval of each cas-symbol is T/N and therefore the bandwidth expansion factor when multiplexing N channels may be roughly N, *the same result as* FDM and TDM/PAM.

A first scheme of the multiplex is showed in the figure 2: The output corresponds exactly to the Galois-Hartley Transform of the "user"-vector $(v_0, v_1, ..., v_{N-1})$. Therefore, it contains all the information about all channels. Each coefficient $V_k$ of the spectrum has duration T/N.

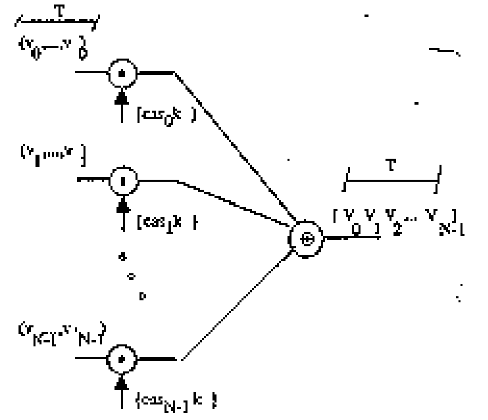



Figure 2. Galois-Field MUX: Spreading sequences.

These carriers can also be viewed as spreading waveforms [MAS 95]. An N-user mux has N spreading sequences, one per channel. The requirements to achieve Welch's lower bound according to Massey and Mittelholzer [MAS&MIT 91], are achieved by $\{cas_i k\}_{k=0}^{p-1}$ sequences. The matrix $[\{cas_i k\}]$ presents both orthogonal rows and orthogonal columns having the same "energy".

A naive example is presented in order to illustrate such an approach (figure 3). A 4-channel mux over GF(5) can be easily implemented i=0,1,...,p-2=3. It is straightforward to see that such signals are not FDMed nor TDMed. GI(5)-valued cas(.) function is shown on table I assuming $\alpha$ equals to 2, an element of GF(5) of order 4.

TABLE I. Cas Function on GI(5) with $\alpha$=2, an element of order 4.

| | | | |
|---|---|---|---|
| $cas_0 0=1+j0$ | $cas_0 1=1$ | $cas_0 2=1$ | $cas_0 3=1$ |
| $cas_1 0=1+j0$ | $cas_1 1=j3$ | $cas_1 2=4$ | $cas_1 3=2j$ |
| $cas_2 0=1+j0$ | $cas_2 1=4$ | $cas_2 2=1$ | $cas_2 3=4$ |
| $cas_3 0=1+j0$ | $cas_3 1=2j$ | $cas_3 2=4$ | $cas_3 3=j3$ |

Putting these results as complex carriers, one has:

$\{cas_0 k\}=\{1,\ 1,\ 1,\ 1\}$
$\{cas_1 k\}=\{1,\ j3,\ 4,\ j2\}$
$\{cas_2 k\}=\{1,\ 4,\ 1,\ 4\}$
$\{cas_3 k\}=\{1,\ j2,\ 4,\ j3\}$.

Therefore, a 4-channel multiplex based on GHT is shown in figure 3.

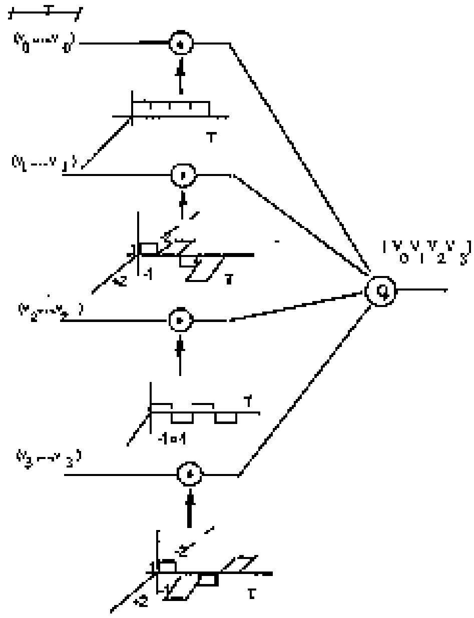



Figure 3. Interpreting Galois-Hartley Transform over GF(5) as spreading waveforms.

The digital carriers are defined on a complex Galois field GI(p) where the element $j=\sqrt{-1}$ may or not may belong to GF(p), although the original definition [CAM et al. 98] considers -1 as a quadratic non residue in GF(p). Two distinct cases are to be considered: p=4k+1 or p=4k+3, k integer. If p = 1 (mod 4), then -1 is a quadratic residue. For instance, considering $j \in GF(5)$ then $2^2=-1 \pmod 5$ so $j=\sqrt{-1}=2 \pmod 5$. Two-dimensional digital $\{cas_i k\}_{k=0}^{p-1}$ carriers then degenerated to one-dimensional carriers.

Considering the above example, carriers are reduced to Walsh carriers!

$\{cas_0 k\}=\{1,\ 1,\ 1,\ 1\}=\{1,1,1,1\}$
$\{cas_1 k\}=\{1,\ 1,\ 4,\ 4\}=\{1,1,-1,-1\}$
$\{cas_2 k\}=\{1,\ 4,\ 1,\ 4\}=\{1,-1,1,-1\}$
$\{cas_3 k\}=\{1,\ 4,\ 4,\ 1\}=\{1,-1,-1,1\}$

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} \Leftrightarrow \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} = \begin{vmatrix} \Delta & \Delta \\ \Delta & -\Delta \end{vmatrix} =$$

[WAL(k,i)].

In the absence of noise, there is no cross-talk from any user to any other one, which corresponds to orthogonal carrier case.

If channels number 1, 2, 3, and 4 are transmitting {4, 0, 1, 2} respectively, the mux output will be (2, 3+4j, 3, 3+j), which corresponds to

{4,0,1,2} ⊗ {1,1,1,1} = 2 mod 5
{4,0,1,2} ⊗ {1,j3,4,j2} = 3+4j mod 5
{4,0,1,2} ⊗ {1,4,1,4} = 3 mod 5
{4,0,1,2} ⊗ {1,j2,4,j3} = 3+j mod 5

There is *no gain* when the transform is taken without alphabet extension. However, we have a nice interpretation of CDM based on finite field transforms.

### 3. A New CDM scheme based on Galois-Hartley Transforms

So far we have essentially considered Finite Field Transforms from GF(p) to GF(p). Extension fields can be used and results are much more interesting: The Galois-Field Division Multiple Access schemes. The advantage of the new scheme named GDMA over FDMA / TDMA regards its higher spectral efficiency.

The new multiplex is carried out over the Galois domain instead the Frequency or time domain. Figure 4 exhibits a block diagram of transform-based multiplexes. First, the Galois spectrum of N-user GF(p) signals is evaluated. The spectral compression is achieved by eliminating the redundancy: only the leaders of cyclotomic cosets are transmitted. The demultiplex is carried out (after signal regeneration) first recovering the complete spectrum by "filling" missing components from the received coset leaders. Then, the inverse finite field transform is computed so as to obtain the demux signals. Another additional feature is that GDM implementations can be made more efficient if fast algorithms for computing the transforms involved are used.

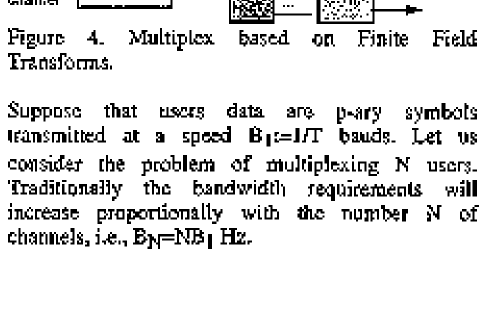



Figure 4. Multiplex based on Finite Field Transforms.

Suppose that users data are p-ary symbols transmitted at a speed $B_I$:=1/T bauds. Let us consider the problem of multiplexing N users. Traditionally the bandwidth requirements will increase proportionally with the number N of channels, i.e., $B_N=NB_I$ Hz.

Thereafter the number of cyclotomic cosets associated with a Galois-Fourier (or Galois-Hartley) finite field spectrum is denoted $v_F$ (respectively $v_H$). The clock driving GHT symbols is N/v times faster than the input baud rate.

__Definition__. The bandwidth compactness parameter $\gamma_{cc}$ is defined as $\gamma_{cc}$: =N/v. ■

It plays a role somewhat similar to the coding asymptotic gain $\gamma_c$ on coded modulation [UNG 82].

Transform-multiplex, i.e., mux based on finite field transforms are very attractive compared with FDM/TDM due to their better spectral efficiency as it can be seen in table II (appendix).

Another point that should be stressed is that instead of compressing spectra (eliminating redundancy), it is possible to use all the coefficients to introduce some error-correction ability. The valid spectrum sequences generate a multilevel block code.

__Lemma 1.__ For an N-user GDMA system over GI($p^m$) with N | $p^m$-1, only a number $v = \gamma_{cc}^{-1}N$ (see below) of finite-field transform coefficients are required to be transmitted.

proof. According to Mœbius' inversion formula, $I_k(q)=\frac{1}{k}\sum_{d|k}\mu(d)q^{k/d}$ gives the number of distinct irreducible polynomials of degree k over GF(q), where μ is the Mœbius function [McE 87]. Therefore, the number $v_F$ of cyclotomic sets on the Galois-Fourier transform $(V_0,V_1,...,V_{N-1})$ is given by

$$v_F=\sum_{k|m}I_k(p)-1.$$

Since each pair of cosets containing reciprocal roots is clustered, then

$$v_H=\frac{v_F-(N \bmod 2)}{2}+1. \qquad ■$$

As a rule-of-thumb, the number of cosets (in fact the gain $\gamma_{cc}$) when N=$p^m$-1 is roughly given by $v_F = \left\lceil \frac{N}{m} \right\rceil$ and $v_H = \left\lceil \frac{1}{2}\left\lceil \frac{N}{m} \right\rceil + 1 \right\rceil$, where $\lceil x \rceil$ is the ceiling function (the smallest integer greater than or equal to x). A simple example over GF(3)→GI($3^3$) is presented below: Factoring $x^{26}$-1 one obtains $v_F$=10 and $v_H$=6. For the FFHT, $V_k^3=V_{26-k3}$ (indexes modulo 26) according to [CAM et al. 98, Lemma 1].

| FFFT cosets | FFHT cosets |
|---|---|
| C0=(0) | C0=(0) |

C1=(1,3,9)
C2=(2,6,18)
C4=(4,12,10)
C5=(5,15,19)
C7=(7,21,11)
C8=(8,24,20)
C13=(13)
C14=(14,16,22)
C17=(17,25,23).

C1=(1,23,9,25,3,17)
C2=(2,6,18,8,24,20)
C4=(4,14,10,22,12,16)
C5=(5,11,19,21,15,7)
C13=(13).

Another interesting possibility is multiplexing without the cyclotomic coset compression. Although such a GDM presents the same spectral efficiency as TDM or FDM it introduces some error-correcting ability yielding a better performance.

By way of interpretation, Hartley transforms can be seen as some kind of Digital Single Side Band since the number of cyclotomic cosets of the FFHT is roughly half that of the FFFT. We can therefore say that *"GDM/FFFT is to FDM/AM as GDM/FFHT is to FDM/SSB."*

Gain of GDM. The gain on the number of channels GDMed regarding to TDM/FDM over the same bandwidth is N-v, which corresponds to $g_{\%}=100(1-\gamma_{cc}^{-1})\%$.
proof. The bandwidth gain is $g_{band}=B_{TDM}/B_{GDM}=\gamma_{cc}$ and the saved Bandwidth is given by $B_{TDM}-B_{GDM}$. Calculating how many additional $B_1$-channels (users) can be introduced:
$(B_{TDM}-B_{GDM})/B_1=(1-\frac{1}{\gamma_{cc}})N.$ ■
In the previous example, a 26-user GDM furnishes a 20-channels gain (≈77%) regarding to TDM.

Indeed, a more formal treatment of spectra should be tried. Power Spectral density calculations must be evaluated by using cyclic Autocorrelation Functions (ACF) of the carriers. As usual, it is assumed that users' data sequences are independent.

Lemma 2. Users' signal sequences can be viewed as wide-sense stationary random processes in both time and Galois-domain, by assuming an uniform probability distribution on GF(p) symbols.
proof.
time domain data stream:
$$\ldots(v_0^{(-1)},v_1^{(-1)},\ldots,v_{N-1}^{(-1)})\,(v_0^{(0)},v_1^{(0)},\ldots,v_{N-1}^{(0)})\,(v_0^{(1)},v_1^{(1)},\ldots,v_{N-1}^{(1)})\ldots$$
Supposing $v_i \in \{0,\pm1,\pm2,\ldots\pm(p-1)/2\}$ equally likely, the mean and the ACF of the discrete process are given respectively by (E denotes the expected value):
$$E\{v_i^{(m)}\}=E\{v_i\}=0 \quad (\forall i), \text{ and}$$
$$R_v(j)=E\{v_i^{(m)}v_{i-j}^{(m)*}\}=E\{v_i\, v_{i-j}^{*}\}=0,\ i\neq j,$$
$$R_v(0)=p^{-1}\left(0+1^2+2^2+3^2+\ldots+(\frac{p-1}{2})^2\right):=P.$$

Galois domain data stream:
$$\ldots(V_0^{(-1)},V_1^{(-1)},\ldots,V_{N-1}^{(-1)})\,(V_0^{(0)},V_1^{(0)},\ldots,V_{N-1}^{(0)})\,(V_0^{(1)},V_1^{(1)},\ldots,V_{N-1}^{(1)})\ldots$$

From $V_k=\sum_{i=0}^{N-1} v_i cas_k i \quad (\forall k)$, it follows that:
$$E\{V_k^{(m)}\}=E\{V_k\}=\sum_{i=0}^{N-1}E(v_i)cas_k i=0 \quad (\forall k).$$
The ACF of the random process (Galois spectrum sequence) is:
$$R_V(j)=E(V_k V_{k-j}^{*})=$$
$$=\sum_{i=0}^{N-1}\sum_{\Delta i=0}^{N-1}E(v_i v_{i-\Delta i}^{*})cas_k i\; cas_{k-j}^{*}(i-\Delta i)$$
$$=\sum_{i=0}^{N-1}\sum_{\Delta i=0}^{N-1}R_v(\Delta i)cas_k i\; cas_{k-j}^{*}(i-\Delta i)$$
$$=R_v(0)\sum_{i=0}^{N-1}cas_k i\; cas_{k-j}^{*} i.$$
From orthogonality properties of $cas_k$ function [CAM et al. 98], it follows that
$R_V(j)=0,\ j\neq 0$ and $R_V(0)=R_v(0).$ ■

This result can be used to show that the multiplex based upon the finite field Hartley transform does not shape the signal power spectrum. Denote by $S_b(t)$ the complex envelope of the generalized QAM (G-QAM) signal s(t), i.e.,
$s(t)=\Re e\{s_b(t)\exp(j2\pi f_c t)\}$ where
$$s_b(t)=\sum_{m=-\infty}^{+\infty}\sum_{k=0}^{N-1}V_k^{(m)}u_{k,m}(t),$$
$$u_{k,m}(t)=u(t-kT-mNT).$$

Theorem 3. The Power Spectral Density of GDM signals is given by $|U(f)|^2$ which depends just on the shape of the spectrum of the shaping filter u(t).
proof. It can be shown that $s_b(t)$ is a cyclostationary process [GAD&FRA 75] but we treat it as a wide-sense stationary one by introducing a random phase uniformly distributed over one block. Therefore we consider a related signal
$$\tilde{s}_b(t)=\sum_{m=-\infty}^{+\infty}\sum_{k=0}^{N-1}V_k^{(m)}u_{k,m}(t;\theta),$$
where $u_{k,m}(t,\theta)=u_{k,m}(t-\theta)$, θ being uniformly distributed in the interval (0,NT). The autocorrelation function (ACF) $R_{\tilde{s}_b}(t,t-\tau)=E\{\tilde{s}_b(t)\tilde{s}_b^{*}(t-\tau)\}$ of the complex envelope is

$$R_{\tilde{s}_b}(t,t-\tau) = \sum_{m=-\infty}^{+\infty}\sum_{\Delta m=-\infty}^{+\infty}\sum_{k=0}^{N-1}\sum_{\Delta k=0}^{N-1} E V_k^{(m)} V_{k-\Delta k}^{(m-\Delta m)*} \frac{1}{NT}\int_0^{NT} u_{k,m}(t,\theta)\, u^*_{k-\Delta k,m-\Delta m}(t-\tau,\theta)\,d\theta$$

where indexes k-Δk are taken mod N.

We first remark that spectra (blocks) are transmitted independently so that complex symbols on different N-vectors are uncorrelated, yielding

$$\sum_{\Delta k=0}^{N-1} E V_k^{(m)} V_{k-\Delta k}^{(m-\Delta m)*} = 0, \quad \Delta m \neq 0.$$

Furthermore, we suppose the sequence of N-dimensional signals is wide-sense stationary (lemma 2) and that there exist a block ACF $R_V(j)$, j=0,1,2,...N-1. The ACF of the complex envelope is therefore

$$R_{\tilde{s}_b}(t,t-\tau) =$$
$$\frac{1}{NT}\sum_{k=0}^{N-1}\sum_{\substack{j=0\\ j\neq k}}^{N-1} R_V(j) \sum_{m=-\infty}^{+\infty}\int_0^{NT} u_{k,m}(t,\theta)\, u^*_{k-j,m}(t-\tau,\theta)\,d\theta$$

By an appropriate change of variables, we obtain

$$R_{\tilde{s}_b}(t,t-\tau) =$$
$$\frac{1}{NT}\sum_{k=0}^{N-1}\sum_{\substack{j=0\\ j\neq k}}^{N-1} E V_k^{(m)} V_{k-j}^{(m)*} \int_{-\infty}^{+\infty} u(\alpha+\tau-kT)\, u^*(\alpha)\,d\alpha$$

Putting the above equation in a simpler notation results in:

$$R_{\tilde{s}_b}(\tau) = R_{\tilde{s}_b}(t,t-\tau) = \frac{1}{NT}\sum_{j=0}^{N-1} R_V(j)\, v(\tau - jT)$$

where $v(\tau - jT) = \int_{-\infty}^{+\infty} u(\alpha + \tau - jT)\, u^*(\alpha)\, d\alpha$.

Indeed, $R_{\tilde{s}_b}(\tau) = \frac{1}{NT} R_V(0)\, v(\tau)$. Taking now the Fourier transform of the ACF, we finally have by the Wiener-Kinchine relation

$S_{\tilde{s}_b}(f) = \frac{P}{NT}|U(f)|^2$, so the power spectrum of the multiplexed signal follows directly from the modulation theorem. ■

What can we say about the alphabet extension? A simple upper-bound on the bandwidth compactness factor can be easily derived. The greatest extension that can be used depends on the signal-to-noise ratio, since the total rate cannot exceed Shannon Capacity over the Gaussian channel. Therefore,

$$B_{GDM}\,\gamma_{cc} \log_2 p \leq B_{GDM} \log_2\left(1+\frac{S}{N}\right) \text{ bps, or}$$

$$\gamma_{cc} \leq \log_p\left(1+\frac{S}{N}\right).$$

## 4. Conclusions

Finite field transforms are offered as a new tool of spreading sequence design. New digital multiplex schemes based on such transforms have been introduced which are *multilevel* Code Division Multiplex. They are attractive due to their better spectral efficiency regarding to classical TDM/CDM which require a bandwidth expansion roughly proportional to the number of channels to be multiplexed. This new approach is promising for cellular mobile communications and channels supporting a high signal-to-noise ratio. Moreover, the Galois-Field Division (GDM) implementation can be easily carried out by a Digital Signal Processor (DSP). Combined multiplex and error-correcting ability should be investigated. Another nice payoff of GDM is that when Hartley Finite Field transforms are used, the mux and demux hardware are exactly the same. It is proved that GDM based on Finite Field Hartley Transform does not shape the signal Power Spectrum. They can directly be applied in multiple access digital schemes.

ACKNOWLEDGMENTS

*This first author expresses his deep indebtness to Professor Gérard Battail whose philosophy had a decisive influence on his way of looking to coding and multiplex.*

REFERENCES

[BLA 79] R.E. Blahut, Transform Techniques for Error Control Codes, *IBM J. Res. Develop*, 23, n.3, pp. 299-314, May, 1979.

[BRI 92] J. Brittain, Scanning the past: Ralph V.L. Hartley, *Proc. IEEE*, vol.80, p. 463, 1992.

[CAM et al. 98] R.M. Campello de Souza, H.M. de Oliveira, A.N. Kauffman and A.J.A. Paschoal, "Trigonometry in Finite Fields and a new Hartley Transform", IEEE *International Symposium on Information Theory*, ISIT, MIT Cambridge,MA, THB4: Finite Fields and Appl., p. 293, 1998. (see http://lids.mit.edu/ISIT98)

[CAM&FAR 85] R.M. Campello de Souza and P.G. Farrel, Finite Field Transforms and Symmetry Groups, *Discrete Mathematics*, 56, pp. 111-116, Elsevier pub., 1985.

[FOR et al. 84] G.D. Forney Jr, R.G. Gallager, G.R. Lang, F.M. Longstaff and S.U. Qureshi, Efficient modulation for Band-limited channels, *IEEE J. Select. Areas Commun.*, SAC 2, Sept., pp. 632-646, 1984

[GAD&FRA 75] W.A. Gadner and L.E. Franks, Characterization of cyclostationary random process, *IEEE Trans. Info. Theory*, 21, Jan., pp. 4-15, 1975.

[HAR 42] R.V.L. Hartley, A more symmetrical Fourier analysis applied to transmission problems, *proc. IRE*, vol 30, pp. 144-150, 1942.

[HON&VET 93] J.J. Hong and M. Vetterli, Hartley Transforms over Finite Fields, *IEEE Trans. Info. Theory*, 39, n.5, pp.1628-1638,Sept.,1993. Also Computing m DFT's over GF(q) with one DFT over GF($q^m$), *IEEE Trans. Info. Theory*, 39, n.1, pp. 271-274, Jan., 1993.

[HOU 87] H.S. Hou, The fast Hartley transform algorithm, *IEEE Trans. Comput.*, vol. 36, pp. 147-156, 1987.

[MAS 95] J.L. Massey, Towards an Information Theory of Spread-Spectrum Systems, in: *Code Division Multiple Access Communications*, Eds S.G. Glisic and P.A. Leppänen, Boston, Dordrecht and London, Kluwer, pp. 29-46, 1995.

[MAS&MIT 91] J.L. Massey and T. Mittelholzer, Welch's bound and sequence sets for Code-Division-Multiple-Access Systems, *Proc. of Sequences'91*, Springer-Verlag, 1991.

[McE 87] R.J. McEliece, Finite Fields for Computer Scientist and Engineers, Kluwer Ac. Pub., 1987.

[POL 71] J.M. Pollard, The Fast Fourier Transform in a Finite Field, *Math. Comput.*, 25, pp. 365-374, Apr., 1971.

[QUAL 92] Qualcomm, The CDMA Network Engineering Handbook, Qualcomm Inc., San Diego, CA, 1992.

[REE et al. 77] I.S. Reed, T.K. Truong, V.S. Kwoh and E.L. Hall, Image Processing by Transforms over a Finite Field, *IEEE Trans. Comput.*, 26, pp. 874-881, Sep., 1977.

[REE&TRU 79] I.S. Reed and T.K. Truong, Use of Finite Field to Compute Convolution, *IEEE Trans. Info. Theory*, pp. 208-213, Mar., 1979.

[SIL&SHA 96] C.A. Siller and M. Shafi, Eds., SONET/SDH: A Sourcebook of Synchronous Networking, IEEE press, 1996.

[UNG 82] G. Ungerboeck, Channel Coding with multilevel/phase signals, *IEEE Trans. Info. Theory*, IT 28, pp. 55-67, Jan., 1982.


**APPENDIX**

TABLE II. A Spectral Efficiency Comparison for Multiplex Systems.

| | one-user | N-users TDMed or FDMed | GDMed |
|---|---|---|---|
| Transmission rate | $R_{l-user} = \frac{\log_2 p}{T}$ | $R = \sum_l R_{l-user} = N\frac{\log_2 p}{T}$ bps | $R = \sum_l R_{l-user} = N\frac{\log_2 p}{T}$ bps |
| Bandwidth requirements | $B_1 = \frac{1}{T}$ Hz | $B_N = \frac{1}{T/N} =$ $NB_1$ Hz | $B_{GDM} = \frac{1}{T/(\gamma_{cc}^{-1}N)}$ $\frac{1}{\gamma_{cc}}(NB_1)$ Hz |
| Spectral efficiency | $\eta_{l-user} = \log_2 p$ bits/s/Hz | $\eta_{mux} = \log_2 p$ bits/s/Hz | $\eta_{GDM} = \gamma_{cc} \log_2 p$ bits/s/Hz |