*Proceedings of IEEE-SP Symposium on Time-Frequency and Time-Scale Methods '92, Victoria, BC*, pages 299–302. IEEE, 1992.

[67] T. Q. Nguyen and P. P. Vaidyanathan. Maximally Decimated Perfect-Reconstruction FIR Filter Banks with Pairwise Mirror-Image Analysis and Synthesis Frequency Responses. *IEEE Trans. on ASSP*, 36(5):693–706, 1988.

[68] J. E. Odegard, R. A. Gopinath, and C. S. Burrus. Optimal Wavelets for Signal Decomposition and the Existence of Scale-Limited Signals. In *Proceedings of the ICASSP '92, San Francisco*. IEEE, March 1992.

[69] L. Pernebo and L.M. Silverman. Balanced Realization of Multivariate Linear Systems. *IEEE Trans. on Automatic Control*, 27:382, 1982.

[70] L. Rabiner and D. Crochière. *Multirate Digital Signal Processing*. Prentice-Hall, 1983.

[71] L. Rabiner and R. W. Schaefer. *Speech Signal Processing*. Prentice-Hall, 1983.

[72] K. R. Rao and P. Yip. *Discrete Cosine Transform - Algorithms, Advantages and Applications*. Academic Press, 1990.

[73] O. Rioul and M. Vetterli. Wavelets and Signal Processing. *IEEE Signal Processing Magazine*, pages 14–37, oct 1991.

[74] W. Rudin. *Real and Complex Analysis*. McGraw-Hill., 3 edition, 1987.

[75] M. J. Smith and T. P. Barnwell. Exact Reconstruction techniques for tree-structured subband coders. *IEEE Trans. on ASSP*, 34:434–441, 1986.

[76] A. K. Soman, P. P. Vaidyanathan, and T. Q. Nguyen. Linear Phase Paraunitary Filter Banks : Theory, Factorizations and Applications. Technical report, California Institute of Technology, May 1992.

[77] H. M. Stark. *An Introduction to Number Theory*. MIT Press, Cambridge, MA, 1989.

[78] P. Steffen. Closed Form Derivation of Orthogonal Wavelet Bases for Arbitrary Integer Scales. Technical report, University of Erlangen-Nürnberg, Germany, 1992.

[79] E. M. Stein and G. Weiss. *Introduction to Fourier Analysis on Euclidean Spaces.* Princeton University Press, Princeton, NJ, 1975.

[80] G. Strang. The Optimal Coefficients in Daubechies Wavelets. *Physica D*, 60:239–244, 1992.

[81] A. H. Tewfik, D. Sinha, and P. Jorgensen. On the Optimal Choice of a Wavelet for Signal Representation. *IEEE Trans. on Information Theory*, 38(2):747–765, Mar 1992.

[82] P. P. Vaidyanathan. Quadrature mirror filter banks, m-band extensions and perfect-reconstruction techniques. *IEEE ASSP Magazine*, pages 4–20, 1987.

[83] P. P. Vaidyanathan. Improved Technique for The Design of Perfect Reconstruction FIR QMF Banks with Lossless Polyphase Matrices. *IEEE Trans. on ASSP*, 37(7):1042–1056, 1989.

[84] P. P. Vaidyanathan. *Mutirate Systems and Filter Banks.* Prentice Hall, 1992.

[85] P. P. Vaidyanathan and Z. Doganata. The Role of Lossless Systems in Modern Digital Signal Processing. *IEEE Trans. on Education*, 32:181–197, August 1989.

[86] P. P. Vaidyanathan and Phuong-Quan Hoang. Lattice Structures for Optimal Design and Robust Implementation of Two-Channel Perfect Reconstruction Qmf banks. *IEEE Trans. on ASSP*, 36(1):81–93, 1988.

[87] P. P. Vaidyanathan and K. Swaminathan. Alias-Free real-coefficient, $M$-band QMF Filter Banks for Arbitrary $M$. *IEEE Trans. on CAS*, 34(12):1485–1496, 1987.

[88] M. Vetterli and Didier Le Gall. Perfect Reconstruction FIR Filter Banks : Some Results and Properties. *IEEE Trans. on ASSP*, 37(7):1057–1071, 1989.

[89] M. Vetterli and C. Herley. Wavelets and Filter Banks: Relationships and New Results. In *Proceedings of the ICASSP '90 Albuquerque, NM*. IEEE, May 1990.

[90] M. Vetterli and C. Herley. Wavelets and Filter Banks : Theory and Design. *IEEE, Trans. on ASSP*, pages 2207–2232, Sept 1992.

[91] M. J. Vetterli. Multirate Filter Banks. *IEEE Trans. on ASSP*, 35:356–372, 1987.

[92] M. Vidyasagar. *Control Systems Synthesis: A Factorization Approach*. MIT Press, 1985.

[93] E. Viscito and J. P. Allebach. The Analysis and Design of Multidimensional FIR Perfect Reconstruction Filter Banks for Arbitrary Sampling Lattices. *IEEE Trans. on Circuits and Systems*, 38:29–42, January 1991.

[94] E. Wigner. Quantum Mechanical Distribution Functions Revisited. In W. Yourgrau and A. van der Merwe, editors, *Perspectives in Quantum Theory*. MIT Press, Cambridge, MA, 1971.

[95] A. Willsky and W. Young. *Signals and Systems*. Prentice Hall, Englewood Cliffs,, 1975.

[96] R. M. Young. *An Introduction to Non-Harmonic Fourier Series*. Academic Press, 1980.

[97] W. R. Zettler, J. Huffman, and D. Linden. The Application of Compactly Supported Wavelets to Image Compression. In *Proceedings of SPIE*, volume 1244, pages 150–160, 1990.

[98] H. Zou and A. H. Tewfik. Discrete Orthogonal $M$-Band Wavelet Decompositions. In *Proceedings of ICASSP, San Francisco, CA*, volume 4, pages IV–605–IV–608. IEEE, 1992.

# Appendix A

# The Aryabhatta/Bezout Identity

A fundamental result in the theory of integer matrices is the Aryabhatta/Bezout identity that arises from the Smith form of integer matrices. First consider the scalar case. For $m, n \in \mathbf{Z}$ let $r = \gcd(m, n)$ and $l = \operatorname{lcm}(m, n)$. Gcds and lcms are are unique modulo multiplication by $\pm 1$, the integers with integer inverse. Now there exist integers $c, d \in \mathbf{Z}$, such that

$$cm = dn = l \quad \text{and} \quad \gcd(c, d) = 1. \tag{A.1}$$

As a consequence of Euclid's algorithm the gcd is also a linear combination of $m$ and $n$ [6]: there exists $a, b \in \mathbf{Z}$, such that

$$r = am + bn \quad \text{and} \quad \gcd(a, b) = 1. \tag{A.2}$$

Unlike $c$ and $d$ (which are unique modulo $\pm 1$) $a$ and $b$ are non-unique. For instance $a$ could be replaced by $a - kn$ and $b$ by $b + kn$ where $k \in \mathbf{Z}$. Also

$$l = \pm mn/r, \tag{A.3}$$

or equivalently $ad + bc = \mp 1$. Eqns. A.1-A.3 summarizes all basic facts about gcds and lcms and can be written in the compact form

$$\begin{bmatrix} a - kn & b + km \\ c & -d \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} \stackrel{\text{def}}{=} U \begin{bmatrix} m \\ n \end{bmatrix} \begin{bmatrix} r \\ 0 \end{bmatrix}, \tag{A.4}$$

with $\det U = \mp 1$ and $k \in \mathbf{Z}$. Notice that $\det U = \pm 1$ is a strong condition and forces $\gcd(a, b) = \gcd(c, d) = 1$. For example when $m = 6$ and $n = 10$, $l = 30$, $g = 2$, $a = 2 - 10k$, $b = 1 + 6k$, $d = 5$, $c = 3$ and $\det U = -1$.

In the matrix case the invertible integer matrices are precisely the unimodular ones. A fundamental fact about integer matrices is the following [49]:

**Fact 10** Every integer matrix $M$ can be written in the form

**Left Hermite Form** $M = UR$, where $U$ is unimodular, lower-triangular, and $R$ is an integer upper triangular matrix

**Right Hermite Form** $M = LV$, where, $V$ is unimodular, upper-triangular, and $L$ is an integer lower triangular matrix

**Smith Normal Form** $M = U\Sigma V$, where $U$ unimodular, lower-triangular, $V$ is unimodular upper-triangular and $\Sigma$ is diagonal. Moreover, the The diagonal elements of $\Sigma$, say $\lambda_i$, can be arranged such that $\lambda_{i+1}|\lambda_i$

### Divisors and Multiples of Integer Matrices

Let $M$, $L$ and $R$ be integer matrices such that $M = LR$. $R$ is a *right divisor* of $M$ and $L$ is a *left divisor* of $M$. Moreover, $M$ is a *left multiple* of $R$ and a *right multiple* of $L$. $R$ is said to be a *common right* divisor of $M$ and $N$ if it is a right divisor of both $M$ and $N$. In this case, $M$ and $N$ must have the same number of columns and there exist integer matrices, $\hat{M}$ and $\hat{N}$ such that $M = \hat{M}R$ and $N = \hat{N}R$.

$M$ is said to be a *left common multiple* of matrices $R_1$ and $R_2$ if $M = L_1R_1$ and $M = L_2R_2$ for some $L_1$ and $L_2$. $M$ is also a *right common multiple* of $L_1$ and $L_2$. Notice that $R_1$ and $R_2$ must have the same number of columns while $L_1$ and $L_2$ must have the same number of rows.

$R$ is a right divisor of $M$ iff $R^T$ is a left divisor of $M^T$. $M$ is a left multiple of $R$ iff $M^T$ is a right multiple of $R^T$. Hence it suffices to talk about right divisors and left multiples only.

### GCRDs/GCLDs and LCLMs/LCRMs

**Definition 16** $R$ is a *greatest common right divisor* (gcrd) of $M$ and $N$ if for every right divisor, $\hat{R}$, of $M$ and $N$ there exists an integer matrix $W$ such that $R = W\hat{R}$.

**Definition 17** $M$ is a *least common left multiple* (lclm) of $R_1$ and $R_2$ if every other left multiple is of the form $\hat{M} = WM$ for some $W$.

**Definition 18** If a gcrd of $M$ and $N$ is unimodular then the matrices are said to be *right coprime*.

**Remark:** If one gcrd is unimodular, all gcrds are unimodular as can be seen (from Definition 16) by comparing determinants.

### Construction of a GCRD and an LCLM

Given $M$ and $N$, the matrix $\begin{bmatrix} M^T & N^T \end{bmatrix}$ can be reduced to its left Hermite form $\begin{bmatrix} R^T & 0 \end{bmatrix}$ (from Fact 10) by a unimodular matrix $U$. $R$ in this construction is a gcrd of $M$ and $N$.

$$U\begin{bmatrix} M \\ N \end{bmatrix} = \begin{bmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{bmatrix}\begin{bmatrix} M \\ N \end{bmatrix} = \begin{bmatrix} R \\ 0 \end{bmatrix}.$$

$$V\begin{bmatrix} R \\ 0 \end{bmatrix} = \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix}\begin{bmatrix} R \\ 0 \end{bmatrix} = \begin{bmatrix} M \\ N \end{bmatrix}.$$

$M = V_{11}R$ and $N = V_{21}R$ and so $R$ is a right divisor. Also $R = U_{11}M + U_{12}N$. For any other right divisor $R_1$, with $M = M_1R_1$ and $N = N_1R_1$,

$$R = [U_{11}M_1 + U_{12}N_1]R_1 \tag{A.5}$$

and therefore $R$ is a gcrd. Also $L = U_{21}N = -U_{22}M$ is an lclm of $M$ and $N$ since $U_{21}$ and $U_{22}$ are left coprime (as we shall shortly see).

**Lemma 35** *(Characterization of Right Coprimeness)* $M$ and $N$ are right coprime iff one of the following is true:

1. $XM + YN = I$ for some integer matrices $X$ and $Y$.
2. The matrix $\begin{bmatrix} M \\ N \end{bmatrix}$ has an integer left inverse.

**Proof:** By coprimeness the gcrd is unimodular and hence from Eqn. A.5 $I = R^{-1}U_{11}M + R^{-1}U_{12}N$. Take $X = R^{-1}U_{11}$ and $Y = R^{-1}U_{12}$. □

The first result is known as called the Bezout identity [49]. The second result says that coprimeness is an invertibility property. For any left invertible (over the integers) integer matrix, any partition of the rows of the matrix gives two right coprime matrices. Coprimeness is a collective property of the rows of $M$ and $N$ (taken together). It also follows (by transposition) that $X^T$ and $Y^T$ are right coprime. Hence $X$ and $Y$ are left coprime. From the unimodularity of $U$ and $V$, $U_{21}V_{12} + U_{22}V_{22} = I$. Hence (from Lemma 35) $U_{21}$ and $U_{22}$ are left coprime that $L$ is an lclm of $M$ and $N$.

All the above results about coprimeness can be summarized results in the following Aryabhatta/Bezout identity over integer matrices. Right coprimeness of $M$ and $N$ is equivalent to the existence of matrices $\tilde{M}$, $\tilde{N}$, $X$, $Y$, $\tilde{X}$ and $\tilde{Y}$ such that

$$\begin{bmatrix} \tilde{Y} & \tilde{X} \\ \tilde{N} & -\tilde{M} \end{bmatrix} \begin{bmatrix} M & X \\ N & -Y \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}.$$

## GCRD/LCLM of sets of matrices

The concepts of gcrds and lclms can be directly generalized to the case of many matrices (provided all of them have the same number of columns). From Lemma 35 computing the gcrd of a set of matrices is the same a computing for just two of them. As for the lclm of a set of say $n$ integer matrices, $M_0, M_1, \ldots, M_{n-1}$, an lclm is obtained recursively. Let $P_i = \text{lclm}(P_{i-1}, M_i)$ with $P_0 = M_0$. Then $P_n$ is an lclm.

# Appendix B

# Form of Modulation in Modulated Filter Banks

Assume that $\epsilon_i$ and $\gamma_i$ (in Eqn. 3.25 and Eqn. 3.26) are linear functions of $i$ of the form

$$\begin{bmatrix} \epsilon_i \\ \gamma_i \end{bmatrix} = \begin{bmatrix} \frac{\pi}{4M}(2i+1)\alpha_2 + \frac{\pi}{2}\beta_2 \\ \frac{\pi}{4M}(2i+1)\alpha_1 + \frac{\pi}{2}\beta_1 \end{bmatrix}.$$

For an MFB to satisfy the PR property we will show that it is necessary that the pairs $(\alpha_1, \alpha_2)$ and $(\beta_1, \beta_2)$ have the same parity. We have PR iff

$$\begin{aligned} f(n_1, n_2) &\stackrel{\text{def}}{=} \sum_{i=0}^{M-1} \sum_n h_i(Mn + n_1) g_i(-Mn - n_2) = \delta(n_1 - n_2) \\ &\stackrel{\text{def}}{=} a_1(n_1, n_2) b_1(n_1, n_2) + a_2(n_1, n_2) b_2(n_1, n_2) \end{aligned}$$

where

$$\begin{bmatrix} a_1(n_1, n_2) \\ a_2(n_1, n_2) \\ b_1(n_1, n_2) \\ b_2(n_1, n_2) \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \sum_n h(Mn + n_1) g(-Mn - n_2) \\ \frac{1}{2} \sum_n (-1)^n h(Mn + n_1) g(-Mn - n_2) \\ \sum_{i=0}^{M-1} \cos\left(\frac{\pi}{2M}(2i+1)(n_1 - n_2 + \frac{\alpha_1 + \alpha_2}{2}) + \frac{\pi(\beta_1 + \beta_2)}{2}\right) \\ \sum_{i=0}^{M-1} \cos\left(\frac{\pi}{2M}(2i+1)(n_1 + n_2 + \frac{\alpha_1 - \alpha_2}{2}) + \frac{\pi(\beta_1 - \beta_2)}{2}\right) \end{bmatrix}.$$

Notice that $a_1(n_1 + M, n_2 + M) = a_1(n_1, n_2)$ and $a_2(n_1 + M, n_2 + M) = a_2(n_1, n_2)$. One can compute the sums $b_1(n_1, n_2)$ and $b_2(n_1, n_2)$ using the fact that

$$\sum_{i=0}^{M-1} \cos((2i+1)u + v) = \begin{cases} \frac{1}{2}\left[\frac{\sin(2Mu+v) - \sin(v)}{\sin(u)}\right] & \text{if } u \neq \pi k \\ M(-1)^k \cos(v) & \text{if } u = \pi k. \end{cases}$$

Indeed

$$b_1(n_1,n_2) = \begin{cases} \frac{1}{2}\left[\frac{\sin(\pi(n_1-n_2+\frac{\alpha_1+\alpha_2}{2})+\frac{\pi(\beta_1+\beta_2)}{2})-\sin(\frac{\pi(\beta_1+\beta_2)}{2})}{\sin(\frac{\pi}{2M}(n_1-n_2+\frac{\alpha_1+\alpha_2}{2})}\right] & \text{if } n_1-n_2+\frac{\alpha_1+\alpha_2}{2} \neq 2Ml. \\ M(-1)^l\cos(\frac{\pi(\beta_1+\beta_2)}{2}) & \text{if } n_1-n_2+\frac{\alpha_1+\alpha_2}{2} = 2Ml. \end{cases}$$

$$b_2(n_1,n_2) = \begin{cases} \frac{1}{2}\left[\frac{\sin(\pi(n_1+n_2+\frac{\alpha_1-\alpha_2}{2})+\frac{\pi(\beta_1-\beta_2)}{2})-\sin(\frac{\pi(\beta_1-\beta_2)}{2})}{\sin(\frac{\pi}{2M}(n_1+n_2+\frac{\alpha_1-\alpha_2}{2})}\right] & \text{if } n_1+n_2+\frac{\alpha_1-\alpha_2}{2} \neq 2Mm \\ M(-1)^m\cos(\frac{\pi(\beta_1-\beta_2)}{2}) & \text{if } n_1+n_2+\frac{\alpha_1-\alpha_2}{2} = 2Mm \end{cases}$$

Consider the FIR case and assume (for simplicity) that $h(n)$ and $g(n)$ are prototypes of length $N = 2Mk$. Then, it is easy to see that $f(n_1,n_2) = \delta(n_1 - n_2)$ implies, for fixed $n_1$, a set of $4Mk - M$ constraints (since outside of a range of extent $4Mk - M$, $h_i(Mn + n_1)$ and $g_i(-Mn - n_2)$ do not overlap) However, since $f(n_1 + M, n_2 + M) = f(n_1,n_2)$, it suffices to consider $n_1 \in \{0, 1, \ldots, M-1\}$ only. Therefore $f(n_1,n_2) = \delta(n_1 - n_2)$ implies a total of $4Mk \times M = 2MN$ constraints. However, this is more than the number of free parameters, $2N$, by a factor of $M$. Hence it is necessary for $b_1(n_1,n_2)$ and $b_2(n_2,n_2)$ to vanish appropriately in order to be able to satisfy the PR constraints. Now we can write $a_1(n_1,n_2)$ as $a_e(n_1,n_2) + a_o(n_1,n_2)$ and $a_2(n_1,n_2)$ as $a_e(n_1,n_2) - a_o(n_1,n_2)$. Then

$$f(n_1,n_2) = a_e(n_1,n_2)(b_1(n_1,n_2) + b_2(n_1,n_2)) + a_o(n_1,n_2)(b_1(n_1,n_2) - b_2(n_1,n_2)).$$

Therefore $b_1(n_1,n_2)$ and $b_2(n_1,n_2)$ have to vanish for all integers that are not a multiple of $2M$. In that case there are $2k - 1$ constraints for fixed $n_1$ for a total of $2Mk - M = N - M$ equations. Clearly this is less than $2N$, the number of free parameters and hence PR is possible. In this case $\alpha_1 + \alpha_2 \in 2\mathbf{Z}$, $\beta_1 + \beta_2 \in 2\mathbf{Z}$, $\alpha_1 - \alpha_2 \in 2\mathbf{Z}$, and $\beta_1 - \beta_2 \in 2\mathbf{Z}$. Therefore the pairs ($\alpha_1$,$\alpha_2$) and ($\beta_1$,$\beta_2$) must be integers of the same parity. Since we can assume $\frac{\pi}{2}\beta_1 \in [0,\pi)$, wlog $\beta_1 = \beta_2 = 0$ or $\beta_1 = \beta_2 = 1$. Choice of $\beta_1 = 1$ merely changes the modulation from cosine to sine (since it is a phase shift of $\frac{\pi}{2}$). Therefore we will assume that $\beta_1 = \beta_2 = 0$. By letting $N$ tend to infinity, one sees that, if $b_1(n_1,n_2)$ and $b_2(n_1,n_2)$ do not vanish as above, then the density of PR constraints is more than the density of free parameters and hence PR is impossible.

With $\beta_1 = \beta_2 = 0$, if we shift the analysis filters to the right by $\frac{\alpha_1+\alpha_2}{2}$ and the synthesis filters to the left by $\frac{\alpha_1+\alpha_2}{2}$ (from Lemma 8 it follows that the PR property is unaffected), and define $\alpha = -\frac{\alpha_1-\alpha_2}{2}$ (since $\alpha_1$ and $\alpha_2$ have the same parity, $\alpha$ is an integer), then for the new filter bank

$$\begin{bmatrix} \epsilon_i \\ \gamma_i \end{bmatrix} = \begin{bmatrix} -\frac{\pi}{4M}(2i+1)\alpha \\ \frac{\pi}{4M}(2i+1)\alpha \end{bmatrix}.$$