CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Glossary of Terms

In general, when a subscript or (non-exponent) superscript is omitted, it should be understood to be N unless otherwise indicated in the text.

General Mathematical Terms

Complex Domain	A subring of the complex numbers.
Cyclotomic	Pertaining to $\mathbb{Z}(\zeta)$ or $\mathbb{Q}(\zeta)$. Appendix A, §3.4, Ch.7
Kronecker product	A type of tensor product, §6.1.1
FFT	Fast Fourier Transform, see Appendix B.
Multiset	A set "counting multiplicities", or an "unordered" sequence.
Quotient Field	Fractions created from ring elements. See [KAP1].
Standard residue	$r \in \mathbb{Z}_n$ is standard if $0 \leq r \leq n-1$.
s.t.	such that
w.l.o.g.	Without Loss Of Generality.
w.r.t.	... with respect to ...

General Mathematical Symbols

$(m;\ i_1, \ldots, i_n)$	$m!/(i_1! \cdots i_n!)$. Multinomial coefficient of the first kind.
$(m;\ i_1, \ldots, i_n)_*$	$m!/(1^{i_1} i_1! \cdots n^{i_n} i_n!)$. Multinomial coefficient of the second kind.
$(x_1, x_2, \ldots, x_n)$	Ideal generated by $x_1, x_2, \ldots, x_n$.
$\langle x_1, x_2, \ldots, x_n \rangle$	(Multiplicative) subgroup generated by $x_1, x_2, \ldots, x_n$.
$\lvert S \rvert$	If S is a set or multiset, the number of elements in S.
$a \,\vert\, b$	a divides b.
$a \parallel b$	a strictly divides b. $a \,\vert\, b$ and $a \neq b$
$\alpha\vert A$, $\alpha\vert_A$	A map α restricted to the set A.
$A^\dagger$	The complex transpose of the matrix A; the adjoint matrix
A^T	The transpose of the matrix A
$A \approx B$	(Group or ring) isomorphism from A to B.
$\binom{n}{m}$	The binomial coefficient, $n!/\left((n-m)!m!\right)$.
$\mathbb{C}$	The complex numbers.
$\mathrm{GL}_n(R)$	The non-singular $n \times n$ matrix group over R.
$\imath$	$\sqrt{-1}$.
I, I_n	The $N \times N$ identity matrix, the $n \times n$ identity matrix.
$\ker_*$	A multiplicative group kernel in a ring.
$\mathrm{M}_n(R)$	The $n \times n$ matrix ring over R.
$\mathbb{N}$	The natural numbers.
$\phi(n)$	The Euler or totient function $= \lvert\mathbb{Z}_n^*\rvert$.
$\mathbb{Q}$	The rationals.
$\mathbb{Q}_\zeta$ or $\mathbb{Q}(\zeta)$	The cyclotomic field containing the primitive root of unity, ζ.
$\mathbb{R}$	The reals.
S_n	The symmetric group on $\mathbb{Z}_n$.
$S_N^{(m)}$	Stirling number of the first kind. §11.6.5
$\mathrm{t}G$	The torsion part of a group G.
$\mathbb{Z}$	The (rational) integers.
$\mathbb{Z}_n$	The ring of remainders modulo n.
$\mathbb{Z}_n^*$	The multiplicative group of coprime residues modulo n.
$\mathbb{Z}_\zeta$ or $\mathbb{Z}(\zeta)$	The cyclotomic integers containing the primitive root of unity, ζ.

Special Terms Used in the Book

Boolean circulant	Circulants over Boolean sets. §9.4
Circulant Space	Either the circulant matrices or circulant vectors.
Eigenspace	R_ζ^N, Q_ζ^N, a vector space enclosing all eigenvalue vectors. §1.8

Filter map	The eigenspace filter map , $\tilde{\Gamma}^n_{mn}$, §3.5.2.
τ Generates v	$v_i = \tau(i) - i,\ \forall i \in \mathbb{Z}_N$. §4.3.5
$[\tau]$ Generates $[v]$	$[v] = [\tau]$. (Also, see $[\tau]$ below.) §4.3.5
Injection map	The circulant or eigenspace injection map, $\tilde{\Gamma}^{mn}_n$, §3.5.2.
Null Multiset	$\sum[v] \equiv 0 \pmod N$. §11.1
Multiplier map	ν_h and $\bar{\nu}_h$, §3.12.
Subrepeating circulant	§5.2
Repetition map	The circulant repetition map, Γ^{mn}_n. §3.5.1
Representer	Given $a \in \mathbf{circ}_n(R)$ its representer is $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. §1.10.1
Residue Class	§3.2.
Residue Class Matrix	§5.1.
s-circulant	Shift-circulant §2.2
Standard basis	$1, \mathrm{u}, \mathrm{u}^2, \ldots, \mathrm{u}^{N-1}$ for $\mathbf{circ}_N$, $e_0, e_1, \ldots, e_{N-1}$ for the eigenspace. 1.10.
Standard circulant	$a \in \mathbf{circ}(\mathbb{R})$ is standard if $\sum_i a_i = 1$ and $a_i \geq 0,\ \forall i$. §9.3.2
Standard Positive	a is standard positive if standard and $a_i > 0,\ \forall i$. §9.3.2
Subscript vector	$v \in {\mathbb{Z}_N}^N$ used as subscripts in a monomial expression,$a_v = a_{v_0} \cdots a_{v_{N-1}}$.
Supercirculant	See Chapter 4.
Wrap-around map	The polynomial map, Γ^N, §3.3. Circulant wrap-around map, Γ^n_{mn}, §3.5.1.
Zero set	A subset, S of $\mathbb{Z}_N$, s.t. $\sum_{i \in S} v_i \equiv 0 \pmod N$. §11.2.3

Special Symbols Used in the Book

$(i)_N$	the principal ideal generated by i in $\mathbb{Z}_N$. §3.2.8
$(i)^*_N$	The residue class set of i mod N. §3.2.8
$\langle\tau\rangle$	The sequence of translations of a permutation $\tau \in S_N$. §11.4
$[v]$	The multiset of components of a vector v. §10.2
$[\tau]$	The multiset of translations of a permutation τ. §10.2
$a_{(m)},\ a^{(m)}$	Subrepeating components. §5.2.6
$\tilde{\alpha}$, α^λ	$\lambda\alpha\lambda^{-1}$ if α is a homomorphism on circulants.
$c(v)$	The circulant determinantal coefficient. (Chapters 4 and 10 only) §4.3
$C(S, v)$	(Chapter 10 only) §11.1.4
C_n	The Kummer units (Chapter 7 only). §7.5.6.4ff
$\overline{C}_p$	Circulant units mapped to cyclotomic units. §7.6.18ff
$\mathbf{circ}_n(R)$	The ring of circulant n-vectors over the ring R. §1.9ff
CIRC_n	The circulant isomorphism $\mathrm{CIRC}_n : \mathbf{circ}_n(R) \mapsto \mathrm{CIRC}_n(R)$. §1.3
$\mathrm{CIRC}_n(R)$	The ring of circulant $n \times n$ matrices with base ring R.
$\Delta_n(a)$	The circulant determinant, $\det \mathrm{CIRC}_n(a)$.
$\Delta_n(A)$	Determinant of a circulant $n \times n$ matrix, $\det(A)$.
δ^N_i	0 if $i \not\equiv 0 \pmod N$, 1 otherwise.
δ_i	δ^N_i when N is assumed known.
δ^n	The idempotent vector numerically equal to $(\delta^n_i)_{i=0,1,\ldots,n-1}$
$\delta^n(x)$	The idempotent map numerically equal to $x\delta^n$ (componentwise product)
$\bar{\delta}^n$	The idempotent circulant numerically equal to $(n/N)\delta^n$. §3.2
$\bar{\delta}^n(x)$	The idempotent map on circulants equal to $\bar{\delta}^n x$. §3.2
D_n	§11.9.1
e_i	A vector in the standard basis for the eigenspace. §1.10
$e_N(x),\ e(x)$	$e^{2\pi\imath x/N}$. (Chapters 4 and 10 only) §4.3.1
E_n	The full group of units in the n^{th} cyclotomic field. (Chapter 7 only) §7.5.6.4
$\bar{E}_p$, $\bar{E}^{\pm}_p$	Subgroup of $\mathbf{circ}_p(\mathbb{Z})$ generated by cyclotomic units. (Chapter 7 only) §7.6.9
F, F_n	The diagonalizing matrix for the circulants. The Fourier matrix. §1.6
$F(v)$	The number of permutations leaving v fixed. (Chapters 4 and 10 only) §4.3.2
γ, γ_+	Inverse λ_1 maps: $\mathbb{Z}_\zeta \to \mathbf{circ}_p(\mathbb{Z})$. §7.6.1, §7.7.3, §7.7.9

γ_-	Related to γ_+. See §7.6.1, §7.7.9
Γ^n	The polynomial wrap-around map. §3.3
Γ_r^s	The circulant wrap-around and/or repeater map. §3.5ff
$\tilde{\Gamma}_r^s$	Injection and/or filter map. §3.5.1 ff
h_+	The class number of the real part of the cyclotomic field.
$H_n(v;\ z)$	The zero-set formula for $c(v)$. §11.2.7
$H_n([v];\ z)$	The multiset formula for $c(v)$. §11.5.3
$K_N(R)$	The shift-circulant matrices over R (Chapter 2 only). §2.2
$L_{n\mid N}$	A subset of the eigenvalue maps, $\{\lambda_n, \lambda_{2n}, \ldots, \lambda_{N-n}\}$ §3.2.12
$L^*_{n\mid N}$	A subset of the eigenvalue maps, $\{\lambda_i \vdash i \in (n)^*_N\}$ §3.2.12
$L_{n\mid N}(c)$	A set of eigenvalues, $\{\lambda_n(c), \lambda_{2n}(c), \ldots, \lambda_{N-n}(c)\}$
$L^*_{n\mid N}(c)$	A set of eigenvalues, $\{\lambda_i(c) \vdash i \in (n)^*_N\}$
$\Lambda_N(R)$	The range of λ which contains $\lambda(\mathbf{circ}_N(R))$. §1.7
λ	The eigenvalue vector map on circulant matrices. §1.7
λ_i	The i^{th} eigenvalue map on circulant matrices. §1.7
	The above can also represent the eigenvalues if the argument is understood.
ℓ_p	A map on $\mathbb{Z}_\zeta \to \mathbb{Z}_p$. §7.2.6
$\bar{\lambda}$	An abbreviated form of the λ map. §7.3.16
μ	A map from $\mathbf{circ}_p(\mathbb{Q})$ to itself. (Chapter 7 only) §7.6.9
N	The default circulant space dimension.
$\mathcal{N}_n(a)$	Algebraic norm in $\mathbb{Q}(\zeta_n)$. §7.2
$\Phi_n(x)$	The n^{th} cyclotomic polynomial of degree $\phi(n)$. §3.4.2
$\mathcal{P}_0(v)$	The set of zero-set partitions of v. §11.2.4
$\mathcal{P}_0([v])$	The set of null multiset partitions of v. §11.5.3
Q	Usually the quotient field of the base ring R of the circulants. §1.8
Q_ζ	The base field of the eigenspace of $\mathbf{circ}_N(R)$. The quotient field of R_ζ. §1.8
$r_n(i)$	Ramanujan sum. §5.1.6 ff.
R	The default symbol for the base ring. Commutative ring with identity.
R_ζ or $R(\zeta)$	The ring formed from R by adding ζ.
R^n	$R \oplus R \oplus \cdots \oplus R$, ($n$ times).
$R[G]$	Group ring formed from the ring R and group G. §3.6
$\mathcal{S}_n$	The full symmetric group on n objects usually taken to be $\{0, 1, \ldots, n-1\}$.
$\mathrm{Stab}(v)$	The set of permutations of a sequence v which leave it fixed.
θ	The defining vector of a $D \in \mathrm{NormCIRC}$. (Chapter 2 only) §2.5
Υ, Υ_c	Ring homomorphism $\mathbf{circ}_N(R) \mapsto R[Z]^N$. §3.6.1
$v : S$	$[v_i \vdash i \in S]$. §11.2.3
U	The circulant matrix $\mathrm{CIRC}(0, 1, 0, \ldots, 0)$. §1.10
u	The circulant vector $(0, 1, 0, \ldots, 0)$ which generates the standard basis. §1.10
$\mathbf{U}(R)$	Group of units of the ring R.
$\mathcal{T}_n$	Trivial units of $\mathbf{circ}_n(\mathbb{Z})$. §7.3.6
$\hat{\mathcal{T}}_n$	$\mathcal{T}_n \cup \hat{\mathcal{T}}_n$ is a finite subgroup of $\mathbf{circ}_n(\mathbb{Q})$. §7.3.6
$\mathcal{U}_n$	The full group of units of $\mathbf{circ}_n(\mathbb{Z})$.
ζ, ζ_n	A primitive N^{th} root of unity, a primitive n^{th} root of unity.
ω	Third root of unity: $\frac{1}{2}(-1 + \imath\sqrt{3})$