Polynomial Residue Systems via Unitary Transforms

Matthew G. Parker[†]

[†]*Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway*
Email: matthew@ii.uib.no
WWW: http://www.ii.uib.no/∼matthew/

Abstract

A polynomial, $A(z)$, can be represented by a polynomial residue system and, given enough independent residues, the polynomial can be reconstituted from its residues by the Chinese remainder theorem (CRT). A special case occurs when the discrete Fourier transform and its inverse realise the residue evaluations and CRT respectively, in which case the residue system is realised by the action of a matrix transform that is unitary. In this paper we generalise the class of residue systems that can be realised by the action of unitary transforms beyond the Fourier case, by suitable modification of the polynomial, $A(z)$. We identify two new types of such system that are of particular interest, and also extend from the univariate to the multivariate case. By way of example, we show how the generalisation leads to two new types of complementary array pair.

1. Polynomial Residue Systems

Let $A(z) = (A_0 + A_1 z + \ldots + A_{N-1} z^{N-1})$ be a univariate polynomial with coefficients $A = (A_0, A_1, \ldots, A_{N-1}) \in \mathbb{C}^N$, for $\mathbb{C}$ the field of complex numbers. One can embed $A(z)$ in a polynomial modulus $M(z)$, where

$$A(z) = A(z) \mod M(z), \qquad \text{iff } \deg(M(z)) \geq N,$$

where $\deg(*)$ is the algebraic degree of $*$. Let $M(z) = \prod_{j=0}^{m-1} m_j(z)$ be the product of m mutually-prime polynomials. Then m residues can be extracted from $A(z)$,

$$A(z) \Leftrightarrow (A(z) \mod m_0(z), A(z) \mod m_1(z), \ldots, A(z) \mod m_{m-1}(z)). \qquad (1)$$

The conversion from left to right in (1) is the evaluation of the residues of $A(z)$ with respect to the residue system described by the factors of $M(z)$. If $\deg(M) \geq N$, and on condition that the $m_j(z)$ are mutually prime, this conversion is invertible, and then the conversion from right to left in (1) is the reconstruction of $A(z)$ from its residues by the Chinese remainder theorem (CRT).

In this paper we are particularly interested in moduli, $M(z)$, which split completely into linear factors, i.e. such that $\deg(M) = m$, in which case the residues of $A(z)$ are complex numbers. Moreover, assuming $m \geq N$, and that $m_j(z) = z - e_j$, the residues can be computed by the action of an $m \times m$ Vandermonde matrix

$$V = \begin{pmatrix} 1 & e_0 & e_0^2 & \dots & e_0^{m-1} \\ 1 & e_1 & e_1^2 & \dots & e_1^{m-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & e_{m-1} & e_{m-1}^2 & \dots & e_{m-1}^{m-1} \end{pmatrix},$$

such that

$$\hat{A} = (A(e_0), A(e_1), \dots, A(e_{m-1}))^t = V\tilde{A},$$

where $\tilde{A} = (A_0, A_1, \dots, A_{N-1}, 0, 0, \dots, 0) \in \mathbb{C}^m$. The CRT can be realised by the action on $\hat{A}$ of the inverse, V^{-1}, of V, which exists if $m \geq N$. Using the formula for the CRT, V^{-1} has the following form,

$$V^{-1} = \begin{pmatrix} h_{0,0} & h_{0,1} & h_{0,2} & \dots & h_{0,m-1} \\ h_{1,0} & h_{1,1} & h_{1,2} & \dots & h_{1,m-1} \\ \dots & \dots & \dots & \dots & \dots \\ h_{m-1,0} & h_{m-1,1} & h_{m-1,2} & \dots & h_{m-1,m-1} \end{pmatrix} \begin{pmatrix} f_0 & 0 & 0 & 0 & 0 \\ 0 & f_1 & 0 & 0 & 0 \\ 0 & 0 & f_2 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & f_{m-1} \end{pmatrix},$$

where $h_j(z) = h_{0,j} + h_{1,j}z + \ldots + h_{m-1,j}z^{m-1} = \frac{M(z)}{m_j(z)}$, and $f_j = (\frac{M(z)}{m_j(z)})^{-1} \mod m_j(z)$.

In general, although V is invertible, it is not unitary, even after normalisation. But it is unitary (after normalisation) for a special case, namely when $M(z) = z^K - \mu$, $|\mu| = 1$, $K \geq N$. For $N|K$ and $M(z) = z^K - 1 = \prod_{k=0}^{K-1}(z - \lambda^k)$, λ a primitive Kth complex root of one, we can realise the residue system by K/N unitary matrices, U_j, $0 \leq j < K/N$, where

$$U_j = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{N-1} \\ \dots & \dots & \dots & \dots & \\ 1 & \alpha^{N-1} & \alpha^{N-2} & \dots & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda^j & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \\ 0 & 0 & 0 & \dots & \lambda^{(N-1)j} \end{pmatrix},$$

and $\alpha = \lambda^{K/N}$, such that

$$\hat{A}_j = \frac{1}{\sqrt{N}}(A(\lambda^j), A(\alpha\lambda^j), \dots, A(\alpha^{N-1}\lambda^j))^t = U_j A. \tag{2}$$

As U_j is unitary, the energy of A equals the energy of $\hat{A}_j$, i.e. $\sum_k |\hat{A}_{j,k}|^2 = \sum_k |A_k|^2$. Finally the CRT can be realised by the action of $U_j^{-1} = U_j^\dagger$ on $\hat{A}_j$, where '†' means transpose-conjugate. This residue system is, of course, the discrete Fourier transform (DFT), and all Fourier spectral points can be approximated to increased precision by increasing K.

The aim of this paper is to extend unitarity characterisation of residue systems beyond the case of the DFT by suitable modification (normalisation) of the polynomial $A(z)$. One motivation here is that unitary transforms preserve energy, as discussed previously, and therefore the

relative magnitudes of the residues take on a stronger meaning if the conversion matrices are unitary. For instance, in the context of spread-spectrum systems, it is desirable that the DFT spectral elements have approximately equal magnitudes. This makes sense precisely because the DFT is unitary. Another motivation is that the use of unitaries facilitate the application of representation theory to residue systems, and vice versa.

We consider only the case where $A(z)$ is a degree-one polynomial, i.e. where $N = 2$, and focus on the case where $\deg(M(z)) = N = 2$. Although quite trivial we are, later, able to say something interesting by tensoring the system n-fold, so as to characterise residue systems for n-variate polynomials.

2. Unitary characterisations for degree-one polynomials

For $N = 2$, $A(z) = A_0 + A_1 z$, and the generic residue evaluation matrix for a modulus, $M(z)$, of algebraic degree 2, is of the form $V = \left(\begin{smallmatrix} 1 & e_0 \\ 1 & e_1 \end{smallmatrix} \right)$. We adjust V to unitary form by normalising each row of V appropriately, and by suitable pairing of e_0 and e_1. Let $e_0 = r\beta \in \mathbb{C}$, $r \in \mathbb{R}$, $|\beta| = 1$, where $\mathbb{R}$ is the field of reals. Then choose $e_1 = \frac{-\beta}{r}$, and create

$$U = \frac{1}{\sqrt{1+r^2}} \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & r\beta \\ 1 & \frac{-\beta}{r} \end{pmatrix}.$$

Whilst U is not V, it is, however, always unitary. Critically - and this is the central point of this paper - the action of U evaluates the residues of a modified form of $A(z)$. Specifically, consider the polynomial

$$A'(z) = \frac{A(z)}{\sqrt{1+\beta^{-2}z^2}}. \tag{3}$$

Then

$$\hat{A}' = (A'(r\beta), A'(\frac{-\beta}{r}))^t = UA.$$

We have generalised the application of unitaries to residue systems beyond the DFT at the price of modifying the polynomial on which we are operating from $A(z)$ to $A'(z)$. Setting $r = 1$ we recover the DFT residue system of (2) for $N = 2$.

As U is unitary, one has an immediate description of the CRT by $U^\dagger$, where

$$U^\dagger = \frac{1}{\sqrt{1+r^2}} \begin{pmatrix} 1 & 0 \\ 0 & r\beta^{-1} \end{pmatrix} \begin{pmatrix} 1 & r \\ 1 & \frac{-1}{r} \end{pmatrix}.$$

Moreover, by writing $\hat{A}(y) = \hat{A}_0 + \hat{A}_1 y$, and

$$\hat{A}'(y) = \frac{\hat{A}(y)}{\sqrt{1+y^2}},$$

we are able to express the CRT as the following evaluation:

$$A = (\hat{A}'(r), \hat{A}'(\frac{-1}{r})\beta^{-1})^t = U^\dagger \hat{A}'.$$

We now identify three types of residue evaluation, as described by U, of particular interest, and characterise the form of U in each case [1, 2]:

- Type I - r fixed: Evaluate $\frac{A(z)}{\sqrt{1+r^2}}$ on the circle $z = r\beta$, $\forall\beta$. As $\sqrt{1+r^2}$ is just a global normalisation, we further restrict to the case $r = 1$, and this evaluation of $\frac{A(z)}{\sqrt{2}}$ on the unit circle recovers the DFT residue system. The evaluations can be realised with respect to pairs $(z = \beta, z = -\beta)$ by the action of unitary, U_I, where

$$U_I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \beta \\ 1 & -\beta \end{pmatrix}.$$

- Type II - $\beta = 1$: Evaluate $\frac{A(z)}{\sqrt{1+z^2}}$ on the real axis $z = r$, $\forall r$. The evaluations can be realised with respect to pairs $(z = r, z = \frac{-1}{r})$ by the action of unitary, U_{II} where, by means of the substitution $r = \tan\theta$,

$$U_{II} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

- Type III - $\beta = i$: Evaluate $\frac{A(z)}{\sqrt{1-z^2}}$ on the imaginary axis $z = ir$, $\forall r$. The evaluations can be realised with respect to pairs $(z = ir, z = \frac{-i}{r})$ by the action of unitary, U_{III} where, by means of the substitution $r = \tan\theta$,

$$U_{III} = \begin{pmatrix} \cos\theta & i\sin\theta \\ \sin\theta & -i\cos\theta \end{pmatrix}.$$

The three unitary characterisations are related as follows. Let

$$\mathcal{N} = \frac{\omega^5}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \qquad \omega = e^{\pi i/4}.$$

$\mathcal{N}$ has multiplicative order 3 and generates a Sylow-3 subgroup, T, of the local Clifford group, C, which has order $3 \times 2^6 = 192$ [3, 1]. We have that

$$U_I = \Delta U_{III}\mathcal{N}, \qquad U_{II} = \Delta' U_I \mathcal{N}, \qquad U_{III} = \Delta'' U_{II}\mathcal{N},$$

where Δ, Δ', and Δ'' are 2×2 unitaries with one non-zero entry per row/column. The post-multiplications by Δ, Δ', and Δ'' do not change spectral magnitudes, so can be ignored if one is focussing on the relative magnitudes of spectral elements. The cyclic subgroup, T, is of importance in the context of the local Clifford group and, moreover, the three members of $T = \{I, \mathcal{N}, \mathcal{N}^2\}$ form a mutually unbiased basis [4] of maximum size 3 for qubits [1] . It is for these reasons that it makes sense to look at the residue systems described by U_I, U_{II}, and U_{III} and, given these justifications, it is interesting that one can link T to residue evaluations on the unit circle, real axis, and imaginary axis, respectively.

[1] The rows of our three matrices are eigenvectors of the Pauli spin matrices, σ_x, σ_y, and σ_z [5].

3. Unitary characterisations for multivariate polynomials

The residue systems in the previous section applied to univariate polynomials of degree one. Things can be made interesting by tensoring up the characteristations n-fold, so as to apply to n-variate polynomials which are of degree-one in each variable.

We consider a multivariate polynomial of the form,

$$\begin{aligned} A(z) &= A(z_0, z_1, \ldots, z_{n-1}) = \textstyle\sum_{k \in \mathbb{F}_2^n} A_k \prod_{j=0}^{n-1} z_j^{k_j} \\ &= A_{0\ldots00} + A_{0\ldots01} z_0 + A_{0\ldots10} z_1 + A_{0\ldots11} z_0 z_1 + \ldots + A_{1\ldots11} z_0 z_1 \ldots z_{n-1}, \end{aligned}$$

with complex coefficients, $A_k \in \mathbb{C}$. Such a structure can be viewed as an n-dimensional array, $A \in (\mathbb{C}^2)^{\otimes n}$, with elements $A_k \in \mathbb{C}$. A third interpretation is to view such a polynomial as a generalised Boolean function, $\mathcal{A}(k) : \mathbb{F}_2^n \to \mathbb{C}$, $k \in \mathbb{F}_2^n$, where $\mathcal{A}(k) = A_k$.

For the three special cases of residue system identified in the previous section we have the following n-fold generalisations [1, 2] where, now, $r \in \mathbb{R}^n$, $\beta = (\beta_0, \beta_1, \ldots, \beta_{n-1})$, $|\beta_j| = 1$, $\forall j$.

- Type I - r fixed: Evaluate $\frac{A(z)}{\prod_{j=0}^{n-1} \sqrt{1+r_j^2}}$ on the n circles $z_j = r_j \beta_j$, $\forall \beta_j, j$. Further restricting to the case $r_j = 1$, $\forall j$, one is evaluating $\frac{A(z)}{2^{n/2}}$ on n unit circles to recover the n-dimensional DFT residue system. The evaluations can be realised, with respect to pairs $(z_j = \beta_j, z_j = -\beta_j)$, by the action on A of unitary, U_I, where

$$U_{I,j} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \beta_j \\ 1 & -\beta_j \end{pmatrix}, \qquad U_I = \bigotimes_{j=0}^{n-1} U_{I,j}.$$

- Type II - $\beta_j = 1\ \forall j$: Evaluate $\frac{A(z)}{\prod_{j=0}^{n-1} \sqrt{1+z_j^2}}$ on the n real axes $z_j = r_j$, $\forall r_j$. The evaluations can be realised, with respect to pairs $(z_j = r_j, z_j = \frac{-1}{r_j})$ by the action on A of unitary, U_{II} where, by means of the substitution $r_j = \tan\theta_j$,

$$U_{II,j} = \begin{pmatrix} \cos\theta_j & \sin\theta_j \\ \sin\theta_j & -\cos\theta_j \end{pmatrix}, \qquad U_{II} = \bigotimes_{j=0}^{n-1} U_{II,j}.$$

- Type III - $\beta_j = i\ \forall j$: Evaluate $\frac{A(z)}{\prod_{j=0}^{n-1} \sqrt{1-z_j^2}}$ on the n imaginary axes $z_j = ir_j$, $\forall r_j$. The evaluations can be realised, with respect to pairs $(z_j = ir_j, z_j = \frac{-i}{r_j})$, by the action on A of unitary, U_{III} where, by means of the substitution $r_j = \tan\theta_j$,

$$U_{III,j} = \begin{pmatrix} \cos\theta_j & i\sin\theta_j \\ \sin\theta_j & -i\cos\theta_j \end{pmatrix}, \qquad U_{III} = \bigotimes_{j=0}^{n-1} U_{III,j}.$$

4. An application for multivariate polynomials

In the context of Fourier analysis it is often desirable that all Fourier spectra are of approximately equal magnitude - energy is spread uniformly over the whole spectrum. We characterise this problem for type I by finding an $A(z)$ such that

$$|A(z)|^2 = A(z)A^*(z^{-1}) \approx \sum_{k\in\mathbb{F}_2^n} |A_k|^2 = \delta, \tag{4}$$

where $z^{-1} = (z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})$, '$P^*(z)$' means conjugate coefficients of $P(z)$, and the generic delta-function, δ, is independent of z. We desire $A(z)$ such that the evaluation of (4) on the n unit circles approximates as closely as possible (in some sense) to δ, this then being the approximate magnitude, at all points, of the Fourier power spectrum of the n-dimensional array, A. It is impossible for (4) to hold exactly, which is why it is written as an approximation. For exactness we have to consider two polynomials instead:

Problem I: Find a pair of n-variate polynomials, $A(z)$ and $B(z)$, such that

$$|A(z)|^2 + |B(z)|^2 = A(z)A^*(z^{-1}) + B(z)B^*(z^{-1}) = \sum_{k\in\mathbb{F}_2^n} (|A_k|^2 + |B_k|^2) = \delta. \tag{5}$$

The answer to Problem I is a called a pair of *complementary arrays* [6, 7, 8].

We propose similar problems for type II and type III scenarios [1, 2]:

Problem II: Find a pair of n-variate polynomials, $A(z)$ and $B(z)$, such that

$$\frac{A(z)A^*(z) + B(z)B^*(z)}{\prod_{j=0}^{n-1}(1+z_j^2)} = 2 = \delta. \tag{6}$$

Problem III: Find a pair of n-variate polynomials, $A(z)$ and $B(z)$, such that

$$\frac{A(z)A^*(-z) + B(z)B^*(-z)}{\prod_{j=0}^{n-1}(1-z_j^2)} = 2 = \delta. \tag{7}$$

We refer to polynomial pairs that satisfy either (6) or (7) as type-II or type-III complementary array pairs, respectively. Given polynomial pairs that satisfy equations (5), (6), or (7), the evaluations of these equations on the complex plane give δ as a residue. In particular, the evaluations have a stronger meaning for z evaluated on the n-fold circle, n-fold real axis, and n-fold imaginary axis, respectively as, in these cases, the residue system is realised by the application of unitary matrices, as discussed previously.

We now provide answers to Problems I, II, and III, to within trivial symmetries, for the case when polynomials $A(z)$ and $B(z)$ have coefficients $\in \{-1, 1\}$. Let $a(k), b(k) : \mathbb{F}_2^n \to \mathbb{F}_2$ be Boolean functions, such that $A_k = \mathcal{A}(k) = (-1)^{a(k)}$, $B_k = \mathcal{B}(k) = (-1)^{b(k)}$. Then [9, 10, 11, 7] the polynomial pair $A(z), B(z)$ satisfy (5) for

$$a(k) = \sum_{j=0}^{n-2} k_j k_{j+1}, \qquad b(k) = a(k) + k_{n-1}.$$

Similarly [1], polynomial pair $A(z), B(z)$ satisfy (6) for

$$a(k) = \sum_{j>l} k_j k_l, \qquad b(k) = a(k) + \sum_j k_j.$$

Finally [1], polynomial pair $A(z), B(z)$ satisfy (7) for

$$a(k) = k_0 \sum_{j=1}^{n-1} k_j, \qquad b(k) = a(k) + k_0 \qquad \text{or} \qquad b(k) = a(k) + k_1 + k_2 + \ldots + k_{n-1}.$$

More general complementary constructions for types II and III, similar to Turyn's construction for type I [12, 13, 8], can be found in [1], and a further construction for type III pairs in [2]. If coefficients of $A(z)$ and $B(z)$ are limited to $\{-1, 1\}$, the solutions to (5) and (6) appear to be unique, to within symmetry. But there are a growing number of solutions for (7) as n increases [2].

Although the above problems/solutions are for n-variate polynomials, both problem and solution can be projected down to the univariate case, whilst preserving coefficient alphabet, as follows. Let $z_0 = y$, $z_j = z_{j-1}^2$, $1 \leq j < n$. Then n-variate polynomials $A(z)$ and $B(z)$ project down to univariate polynomials $A(y)$ and $B(y)$ of algebraic degree $2^n - 1$, and problems of type I, II, and III, are projected down to the problem of finding $A(y)$ and $B(y)$ such that

$$A(y)A^*(y^{-1}) + B(y)B^*(y^{-1}) = \delta, \qquad [6]$$

$$\frac{A(y)A^*(y) + B(y)B^*(y)}{\sum_{j=0}^{2^n-1} y^{2j}} = \delta,$$

$$\frac{A(y)\breve{A}^*(y) + B(y)\breve{B}^*(y)}{\prod_{j=0}^{n-1}(1 - y^{2^{j+1}})} = \delta,$$

respectively, where $\breve{P}(y) = \sum_{j=0}^{2^n-1} P_j(-1)^{\mathrm{w}(j)} y^j$, and $\mathrm{w}(j)$ means binary weight of j. The corresponding solutions are given by projection of solutions for the multivariate case [7].

5. Conclusion

By modification of polynomial forms, we have generalised the application of unitary matrix transforms to residue systems other than the discrete Fourier transform. We have characterised unitaries for the case where the polynomials are of degree one, and these characterisations lead us to identify three types of residue system of particular interest. Residue systems for n-variate polynomials can then be realised by the application of n-fold tensor products of these unitaries. For such systems we characterise the problem of finding complementary array pairs of types I, II, and III, and give solutions for the case where all coefficients are in $\{1, -1\}$. Finally, we show how problems/solutions for an n-variate system can be projected down to problems/solutions for a univariate system. Further directions include an investigation of more general types of residue system, as characterised by unitaries in this paper, and finding unitary characterisations for polynomials of degree greater than one. Another direction is to consider problems other than complementary pairs.

References

[1] Matthew G. Parker, Close encounters with Boolean functions of three different kinds, 2nd International Castle Meeting on Coding Theory and Applications, 2ICMCTA, Castillo de la Mota. Medina del Campo (Valladolid), *Lecture Notes in Computer Science* LNCS 5228 September (2008), 15–19. http://www.ii.uib.no/∼matthew/Encounters.pdf

[2] Tor E. Bjørstad, Matthew G. Parker, Equivalence Between Certain Complementary Pairs of Types I and III, in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes* Volume 23, NATO Science for Peace and Security Series - D: Information and Communication Security, Edited by: B. Preneel, S. Dodunekov, V. Rijmen and S. Nikova, June (2009). http://www.ii.uib.no/∼matthew/CompEquivCorrected.pdf

[3] Constanza Riera, Matthew G. Parker, Generalised Bent Criteria for Boolean Functions (I), *IEEE Trans Inform. Theory* **52** 9 Sept. (2006), 4142–4159.

[4] J. Schwinger, Unitary Operator Bases, *Proc Nat. Acad. Sci. U.S.A.* **46** (1960), 560.

[5] P. Šulc, J. Tolar, Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions, *J. Phys. A: Math. Theor.* **40** 15099 (2007).

[6] M.J.E. Golay, Multislit spectroscopy, *J. Opt. Soc. Amer.* **39** (1949), 437–444.

[7] Jonathan Jedwab and Matthew G. Parker, Golay Complementary Array Pairs, *Designs, Codes and Cryptography* **44** July (2007), 209–216.

[8] Frank Fiedler, Jonathan Jedwab, Matthew G. Parker, A Multi-dimensional Approach to the Construction and Enumeration of Golay Complementary Sequences, *J. Combinatorial Theory (Series A)* **115** (2008), 753–776.

[9] J.A. Davis, J. Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, *IEEE Trans. Inform. Theory* **45** (1999), 2397–2417.

[10] M.G. Parker, C. Tellambura, A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio, *Int. Symp. Information Theory, Lausanne, Switzerland* June 30–July 5, (2002), 239.

[11] M.G. Parker, C. Tellambura, A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio, *Reports in Informatics, University of Bergen* Report No 242, ISSN 0333–3590, February (2003). http://www.ii.uib.no/∼matthew/ConstructReport.pdf

[12] R.J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory (A)* **16** (1974), 313–333.

[13] P.B. Borwein, R.A. Ferguson, A complete description of Golay pairs for lengths up to 100, *Mathematics of Computation* **73** 967985 (2003).