Fibonacci Designs

Harold N. Ward
Department of Mathematics
University of Virgnia
Charlottesville, VA 22903
USA
hnw@virginia.edu

Version: April 14, 2010

Abstract: A Metis design is one for which $v = r + k + 1$. This paper deals with Metis designs that are quasi-residual. The parameters of such designs and the corresponding symmetric designs can be expressed by Fibonacci numbers. Although the question of existence seems intractable because of the size of the designs, the nonexistence of corresponding difference sets can be dealt with in a substantive way.

We also recall some inequalities for the number of fixed points of an automporphism of a symmetric design and suggest possible connections to the designs that would be the symmetric extensions of Metis designs.

Key Words: quasi-symmetric design, symmetric design, Metis design, Fibonacci numbers, automorphism.
2010 Mathematics Subject Classification: Primary: 05B05, 05B10; Secondary: 11B39

1. QUASI-RESIDUAL METIS DESIGNS

In the paper [16] by McDonough, Mavron, and the author, a method of amalgamating nets and designs was presented that led to quasi-symmetric designs similar to those discovered by Bracken, McGuire, and the author [3]. At various stages of the construction, restrictions on the designs involved needed to be imposed in order to make the final amalgamation have desired regularity properties. One particular type of design was a generalization of Hadamard designs, and we named them *Metis designs*, in honor of Hadamard's ancestral home, Metz. They are block designs whose standard parameter set (v, b, r, k, λ) satisfies the additional relation $v = r + k + 1$. Symmetric Metis designs are indeed Hadamard designs. The family of Metis designs $\mathcal{M}$ has the following property: regard the parameter set for any design as a point in $\mathbb{R}^5$ on the variety $\mathcal{D}$ defined by the two standard design relations $vr = bk$ and $r(k-1) = \lambda(v-1)$. Then if a design belongs to $\mathcal{M}$, there is a line in $\mathcal{D}$ through the corresponding point such that all the points on that line satisfy the relation defining $\mathcal{M}$. There are other common families of designs with such a linear property. The nature of lines in $\mathcal{D}$ has been explored in the somewhat speculative preprint [22]. For example, the parameter set of a design that is not degenerate in a certain sense lies on four lines in $\mathcal{D}$.

It seems a natural question to ask for Metis designs that are also quasi-residual. The parameters would satisfy the two equations

$$\begin{aligned} v &= r + k + 1 \\ r &= k + \lambda, \end{aligned}$$

along with the two standard equations. Solving the four equations in terms of r, we get $k = (\sqrt{(5r+4)r} - r)/2$. Let $d = \gcd(5r+4, r)$. Then $d|4$, and $(5r+4)/d$ and r/d must separately be squares. Reading modulo 4, we find that $d = 2$ will not work, and so $d = 1$ or 4. Then $5r+4$ and r themselves must be squares. Put $5r+4 = x^2$ and $r = y^2$, with $x, y > 0$. Let F_t and L_t be the t-th Fibonacci and Lucas numbers, respectively, starting with $F_0 = 0$ and $L_0 = 2$ (see the books by Koshy [13] or Vajda [20], for example, which were sources for several of the citations). One has

Lemma 1. *[15, Lemma 2] For some $t \geq 1$, $x = L_{2t}$ and $y = F_{2t}$.*

We substitute these values for x and y in the design parameters, make use of the relation $L_{2t} = F_{2t+1} + F_{2t-1}$ [20, Formula (6)], and invoke the basic recurrence $F_{t+2} = F_{t+1} + F_t$, to obtain

$$v = F_m F_{m-1} + 1,\ b = F_{m+1} F_{m-1},\ r = F_{m-1}^2,\ k = F_{m-1} F_{m-2},\ \lambda = F_{m-1} F_{m-3},$$

where m is odd. The parameters (v', k', λ') for a symmetric design having the Metis design as its block residual are $v' = b' = b + 1$, $r' = k' = r$, and $\lambda' = \lambda$. By the relation $F_{m+1} F_{m-1} + 1 = F_m^2$ [20, Formula (29)],

$$v' = F_m^2,\ k' = F_{m-1}^2,\ \lambda' = F_{m-1} F_{m-3}.$$

The order of this design is $n' = k' - \lambda' = F_{m-1}^2 - F_{m-1} F_{m-3} = F_{m-1} F_{m-2}$. Prompted by the appearance of the Fibonacci numbers, we call a symmetric design $\mathcal{F}_m$ with parameters $(v', k', \lambda') = (F_m^2, F_{m-1}^2, F_{m-1} F_{m-3})$, m odd, a *Fibonacci design.* As we shall concentrate on these symmetric designs, we drop the dashes for clarity.

2. EXISTENCE OF FIBONACCI DESIGNS

The design $\mathcal{F}_3$ is the trivial $(4, 1, 0)$ design whose blocks are the singleton sets, so we may assume that $m > 3$ (m always odd) from now on. There are 78 inequivalent $(25, 9, 3)$ designs $\mathcal{F}_5$, a classification due to Denniston [7]. The first such design was presented by Bhattacharya [1], and an $\mathcal{F}_5$ appears as one of the sequence of designs constructed by Mitchell [17].

The initial step is to check whether the parameter set passes the Bruck-Ryser-Chowla criterion (see, for example, [9, Theorem 10.3.1]). The variety parameter $v = F_m^2$ is even just when m is also divisible by 3, that is, when $m \equiv 3 \pmod 6$. This is a consequence of the periodicity of the F_t modulo any given integer; see [21] for generalities. In this case, the demand is that the order $F_{m-1} F_{m-2}$ be a square. As consecutive Fibonacci numbers are relatively prime [20, p. 73], both F_{m-1} and F_{m-2} would have to be squares. But for $t > 0$, F_t is a square just at $t = 1, 2, 12$ [6]. Thus the only existing design with v even is $\mathcal{F}_3$.

Now suppose that v is odd, so that $m \equiv \pm 1 \pmod 6$. Then $v = F_m^2 \equiv 1$ (mod 4), and the Diophantine equation of the Bruck-Ryser-Chowla theorem is

$$Z^2 = nX^2 + \lambda Y^2 = F_{m-1} F_{m-2} X^2 + F_{m-1} F_{m-3} Y^2.$$

Here there is an easy solution: $X = Y = 1$ and then $Z = F_{m-1}$!

2.1. Difference set development

With that obstacle to existence removed for $m \equiv \pm 1 \pmod 6$, how might one construct $\mathcal{F}_m$? A natural thing to try is to produce $\mathcal{F}_m$ as the development of a difference set ("development" for short). In what follows, z^* is the square-free part of the integer z.

THEOREM 1. *Suppose that $\mathcal{F}_m$ is the development of a difference set in a group (Abelian or not), with $m \equiv \pm 1 \pmod 6$. Let p be a prime dividing F_m. Then any prime dividing either F^*_{m-1} or F^*_{m-2} has odd order modulo p. Moreover, $p \equiv 1 \pmod 8$.*

Proof. The theorem is a consequence of [14, Theorem 4.4], which can be paraphrased in the present situation to say that for no prime p dividing v is there a prime dividing n^* that has even order modulo p. As $v = F_m^2$, such p are the prime divisors of F_m. Because F_{m-1} and F_{m-2} are relatively prime, $n^* = F^*_{m-1}F^*_{m-2}$, and the primes dividing n^* are those dividing either F^*_{m-1} or F^*_{m-2}. Thus such primes must have odd order modulo p. Now $F^2_{m-1} + 1 = F_m F_{m-2}$, by [20, Formula (29)] again. Put $F_{m-1} = a^2 F^*_{m-1}$. Then $a^4(F^*_{m-1})^2 \equiv -1 \pmod p$. Since all the primes dividing F^*_{m-1} must have odd order modulo p, F^*_{m-1} itself has odd order modulo p. Thus if u is the odd factor of $p-1$, then $(a^u)^4 \equiv -1 \pmod p$. Hence the multiplicative group of $\mathbb{Z}_p$ has order divisible by 8, making $p \equiv 1 \pmod 8$. ∎

COROLLARY 1. *If $\mathcal{F}_m$ is a development for some m with $m \equiv \pm 1 \pmod 6$, then in fact $m \equiv \pm 1 \pmod{12}$.*

Proof. By the observation on square Fibonacci numbers, $n^* \neq 1$. From the theorem, all prime divisors p of F_m have $p \equiv 1 \pmod 8$, so that $F_m \equiv 1 \pmod 8$. The period of congruences modulo 8 of the F_t is 12, and the residue sequence is

$$0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, 1, \ldots.$$

Thus $m \equiv \pm 1 \pmod{12}$. ∎

For instance, suppose, indeed, that $m \equiv \pm 1 \pmod{12}$. When 5 divides m, 5 also divides F_m. So if $m \equiv \pm 25 \pmod{60}$, then $m \equiv \pm 1 \pmod{12}$ all right; but F_m has the prime divisor $5 \not\equiv 1 \pmod 8$, and no $\mathcal{F}_m$ can be a development.

Even if all primes p dividing F_m do have $p \equiv 1 \pmod 8$, *every* prime dividing F^*_{m-1} or F^*_{m-2} must have odd order modulo such p if $\mathcal{F}_m$ is a development. Here is a consequence:

THEOREM 2. *Let $m \equiv 1 \pm 36 \pmod{216}$. Then no $\mathcal{F}_m$ is a development.*

Proof. Here $m - 1 = 36(6h \pm 1)$ for some h. By Lucas' law of repetition, as given more sharply in [5, Theorem X] (referenced in [19, p. 13]), the exact power of 3 dividing F_{m-1} is 3^3, the exact power dividing F_{36}. Thus $3 | F^*_{m-1}$. In addition, $m \equiv 5 \pmod 8$ gives $F_m \equiv 2 \pmod 3$, from the sequence $0, 1, 1, 2, 0, 2, 2, 1, 0, \ldots$ of remainders of F_t modulo 3. Thus for some prime p dividing F_m, $p \equiv 2 \pmod 3$, so that $\left(\frac{p}{3}\right) = -1$. If an $\mathcal{F}_m$ is a development, Theorem 1 implies that $p \equiv 1 \pmod 8$. Then $\left(\frac{3}{p}\right) = -1$, from quadratic reciprocity. But that means 3 cannot have odd order modulo p. ∎

There is a similar approach for the $m \equiv -1 \pmod{12}$, for which 2 is a divisor of F^*_{m-2}. If 2 has even order modulo F_m, then for some prime p dividing F_m, 2 will also have even order modulo p, and a development model for $\mathcal{F}_m$ will be ruled out. The computation of the order is rather formidable, and the m for which this works do not seem to follow an obvious pattern. The first few are $m = 35$, 47, 59, 71, 95, 107, 119, 143, 155, 167, 191, and 203. (In point of fact, $m = 35$, 95, 119, 143, 155, and 203 are also ruled out for $\mathcal{F}_m$ developments by prime factors of F_m not congruent to 1 modulo 8.)

We have $F_{m-1}^2 \equiv -1 \pmod{F_m}$, and in addition, $F_{m-2}^2 \equiv -1 \pmod{F_m}$, since $F_{m-2} \equiv -F_{m-1} \pmod{F_m}$. Thus if an $\mathcal{F}_m$ is a development and either of F_{m-1} or F_{m-2} is square-free, one of these congruences is contradicted by the fact that F_{m-1}^* and F_{m-2}^* must have odd order modulo any prime divisor of F_m. Such a contradiction is in fact what happens for all $m \equiv \pm 1 \pmod{12}$ with $m < 1000$, except for $m = 277$, 457, 577, and 877. (The web page by B. Kelly [11] contains factorizations of the first thousand Fibonacci numbers, along with tables that can be used for the first *ten* thousand.) For the first three of these m, the possibility that $\mathcal{F}_m$ exists as a development is ruled out by a factor of F_m not congruent to 1 modulo 8. For $m = 877$, the prime 1753 divides F_{877}, and F_{875} is exactly divisible by 5^3. Thus 5 is in the square-free part of F_{875}. As the order of 5 modulo 1753 is 584, the odd-order requirement does not hold. In short, no $\mathcal{F}_m$ for $m \equiv \pm 1 \pmod{12}$ with $m < 1000$ can be a development. That $\mathcal{F}_5$ is not one is recorded in [14, Table 4-1]; and that a $(169, 64, 24)$ design $\mathcal{F}_7$ cannot be a development is presented in [12]. Whether such a design exists at all seems to be unknown.

All of these results suggest the conjecture that apart from the trivial design $\mathcal{F}_3$, no Fibonacci design is a development of a difference set–and this seems to depend on mysterious properties of Fibonacci numbers.

3. BOUNDS

A standard approach to constructing symmetric designs is to prescribe a group of automorphisms, thereby limiting the choices needed to be explored in the construction. The investigation of the possible orbit structure of an automorphism of specified order is an important starting point. The fact that the cycle structures of the permutations induced on the points and blocks by an automorphism are the same [18] is a key ingredient.

There are various bounds on the number of fixed points of an automorphism of a symmetric design; some are summarized and proved in [14, Section 3.1]. We shall present one due to Bowler [2, Lemma 2.5 (i)] with essentially his proof. This bound was later generalized by Feit [8].

THEOREM 3. *The three-block bound: Let σ be an automorphism of a symmetric (v, k, λ) design $\mathcal{D}$ of order $n = k - \lambda$, and let σ have f fixed points. Then if the order of σ is at least 3, $f \leq v - 3n$.*

Proof. Take l to be the length of a longest cycle in the action of σ on the blocks of $\mathcal{D}$, and let B_1, B_2, and B_3 be three distinct blocks in that cycle. With $|X|$ denoting the size of a set X, we have $|B_1 \cup B_2 \cup B_3| = 3k - 3\lambda + |B_1 \cap B_2 \cap B_3|$. Since any fixed point of σ in one of the B_i is in all three, there are no fixed points in $B_1 \cup B_2 \cup B_3 - B_1 \cap B_2 \cap B_3$. Thus

$$f \leq v - |B_1 \cup B_2 \cup B_3 - B_1 \cap B_2 \cap B_3| = v - 3(k - \lambda) = v - 3n.$$

∎

Suppose that equality holds in the three-block bound: $f = v - 3n$. Continue with the notation in the proof, and let B be a representative block in the chosen longest cycle of σ. Then the complement of $B_1 \cup B_2 \cup B_3 - B_1 \cap B_2 \cap B_3$ is the set F of fixed points of σ; and $B_1 \cap B_2 \cap B_3$ must be the set F_0 of fixed points in B, which is the set of fixed points in each B_i. The set $W = B_1 \cup B_2 \cup B_3 - B_1 \cap B_2 \cap B_3$ is the union of all the orbits of σ other than the fixed points. Each such orbit must accordingly have a point in B. Moreover, B cannot contain a complete such orbit, for then it would be in all the B_i and so in $B_1 \cap B_2 \cap B_3$ and yet not consist of fixed points. In particular, σ cannot have a cycle with length $t > 1$ and relatively prime to l. Because $W = B_1 \cup B_2 \cup B_3 - B_1 \cap B_2 \cap B_3$, $B_3 \supseteq F_0 \cup (W - (B_1 \cup B_2))$. With $|F_0| = f_0$, then since $|W| = 3n$ and F_0 is disjoint from W, $|F_0 \cup (W - (B_1 \cup B_2))| = 2f_0 + k - 2\lambda$. If $l \geq 4$, the same holds for a fourth block B_4 in the orbit, in place of B_3. Then $B_3 \cap B_4 \supseteq F_0 \cup (W - (B_1 \cup B_2))$, so that $\lambda \geq 2f_0 + k - 2\lambda$, and $f_0 \leq k - 3n/2$.

Assume now that $l \geq 5$. If B contains a point x in a 2-cycle of σ, then $x \in B \cap B^{\sigma^2} \cap B^{\sigma^4}$ but $x \notin F_0$. Similarly, if x and y are together in a 3- or 4- cycle of σ and in B, then with proper choice of the B_i, one would find $x \in B_1 \cap B_2 \cap B_3$. So 2-cycles of σ on points do not meet B at all, and 3- or 4- cycles meet B at most once. Likewise, if $x, y, z \in B$ are in a common t-cycle of σ with $t \geq 5$, then as $t \leq l$, $x \in B_1 \cap B_2 \cap B_3$ for certain B_i. Thus a t-cycle of σ with $t \geq 5$ meets B at most twice.

Now let c_t be the number of t-cycles of σ for $t > 1$. Then the preceding considerations give

$$k \leq f_0 + c_3 + c_4 + 2\sum_{t \geq 5} c_t. \tag{1}$$

Since $v = f + \sum_{t \geq 2} tc_t$, we have

$$3n = v - f = \sum_{t \geq 2} tc_t \geq 5/2(c_3 + c_4 + 2\sum_{t \geq 5} c_t). \tag{2}$$

Therefore $f_0 \geq k - 6n/5$. But $f_0 \leq k - 3n/2$, and that is a contradiction. Thus:

Corollary 2. *If equality holds in the three-block inequality, then the length l of the longest cycle in σ is at most 4. Moreover, the order of σ is l.*

The order statement follows from the comment that cycle lengths greater than 1 must be relatively prime to l.

It is not hard to find designs with automorphisms of order 3 or 4 meeting the three-block bound. For example, let Q be a normalized Hadamard matrix of order 4 (see any of [9, 10, 14], for instance). It has an automorphism of order 3 fixing the first row and first column. If H is an Hadamard matrix of order h, then the Kronecker product $Q \otimes H$ inherits an automorphism of order 3 fixing the first h rows and columns. The corresponding Hadamard design is a $(4h-1, 2h-1, h-1)$ symmetric design of order h with an automorphism of order 3 having $h-1 = (4h-1)-3h$ fixed points. Similarly, a normalized Hadamard matrix E of order 8 has an automorphism of order 4 fixing the first two rows and columns, switching the third and fourth, and cycling the last four (on proper ordering; this may be seen from the construction of E as a Sylvester matrix). Then $E \otimes H$ leads to an $(8h-1, 4h-1, 2h-1)$ Hadamard design of order $2h$ having an automorphism of order 4 with both 2-cycles and 4-cycles and $2h - 1 = (8h - 1) - 3 \times (2h)$ fixed points.

Our interest here is that appropriate Fibonacci designs may be candidates for designs with automorphisms meeting the three-block bound. Unfortunately, there is not much evidence! The design $\mathcal{F}_3$ has an automorphism of order 3 with $1 = 4-3\times 1$ fixed points. More interestingly, several $\mathcal{F}_5$ designs can be constructed to have an automorphism of order 3 with $7 = 25 - 3\times 6$ fixed points. Thus in the notation of [1], Bhattacharya's design has the automorphism

$$(X_1Y_1Z_1)(X_2Y_2Z_2)(X_3Y_3Z_3)(X_4Y_4Z_4)(V_1V_2V_3)(W_1W_3W_2)$$

on points.

So can such an $\mathcal{F}_7$, that is, a $(169, 64, 24)$ design, be created? It is tantalizing to observe that the parameters of the $(41, 16, 6)$ design constructed by Bridges, Hall, and Hayden [4] (which, in fact, has an automorphism of order 3 with $11 = 41-3\times 10$ fixed points) and $(169, 64, 24)$ are given by $t = 2$ and $t = 3$ in the sequence

$$v = \frac{2q(q^t-1)}{q-1} + 1,\ k = q^t,\ \lambda = \frac{1}{2}q^{t-1}(q-1)$$

for $q = 4$. This same parameter sequence, but with q a power of an *odd* prime, corresponds to a family of designs discovered by A. E. Brower that is presented in [10, Section 11.8]. Incidentally, this parameter set does not always pass the Bruck-Ryser-Chowla test. One has $n = q^{t-1}(q+1)/2$ and $v \equiv 1 \pmod 4$, so the Diophantine equation is

$$2Z^2 = q^{t-1}((q+1)X^2 + (q-1)Y^2).$$

If q is an even power of 2 or t is even, this has the solution $X = 1, Y = 1, Z = \sqrt{q^t}$. If neither condition holds, q^{t-1} is a square that can be absorbed into X^2 and Y^2. The solvability criterion of Legendre here comes down to the requirement that -1 be a square modulo each prime divisor p of $(q+1)^*$ (see [14, pp. 45–46], among others); that is, that $p \equiv 1 \pmod{4}$. For odd powers q of 2, it is a pleasant exercise to show that only $q = 8$ passes: $2\times 12^2 = 9\times 5^2 + 7\times 3^2$.

REFERENCES

[1] K. N. Bhattacharya, *On a new symmetrical balanced incomplete block design,* Bull. Calcutta Math. Soc., **36** (1944), 91–96.

[2] A. Bowler, *On the fixed points of an automorphism of a symmetric design,* Discrete Math., **138** (1995), 119–124.

[3] C. Bracken, G. McGuire, and H. N. Ward, *New quasi-symmetric designs constructed using mutually orthogonal Latin squares and Hadamard matrices,* Des. Codes Cryptogr., **41** (2006), 195–198.

[4] W. G. Bridges, M. Hall, Jr., and J. L. Hayden, *Codes and designs,* J. Combin. Theory Ser. A, **31** (1981), 155–174.

[5] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$,* Ann. of Math., **15** (2) (1913–1914), 30–70.

[6] J. H. E. Cohn, *On square Fibonacci numbers,* J. London Math. Soc., **39** (1964), 537–540.

[7] R. H. F. Denniston, *Enumeration of symmetric designs* $(25, 9, 3)$, "Algebraic and Geometric Combinatorics," North-Holland Math. Stud. **65**, North-Holland, Amsterdam, 1982; pp. 111–127.

[8] W. Feit, *Automorphisms of symmetric balanced incomplete block designs,* Math. Z., **118** (1970), 40–49.

[9] M. Hall, Jr., "Combinatorial Theory," 2nd ed., Wiley-Interscience, New York, 1986.

[10] Y. J. Ionin and M. S. Shrikhande, "Combinatorics of Symmetric Designs," New Mathematical Monographs, **5**, Cambridge University Press, Cambridge, 2006.

[11] B. Kelly, *Fibonacci and Lucas Factorizations,*
http://home.att.net/~blair.kelly/mathematics/fibonacci/

[12] L. E. Kopilovich, *Difference sets in noncyclic abelian groups,* Cybernetics, **25** (1989), 153–157.

[13] T. Koshy, "Fibonacci and Lucas Numbers with Applications," Wiley-Interscience, New York, 2001.

[14] E. S. Lander, "Symmetric Designs: an Algebraic Approach," London Mathematical Society Lecture Note Series, **74**, Cambridge University Press, Cambridge, 1983.

[15] C. T. Long and J. H. Jordan, *A limited arithmetic on simple continued fractions,* Fibonacci Quart., **5** (1967), 113–128.

[16] T. P. McDonough, V. C. Mavron, and H. N. Ward, *Amalgams of designs and nets,* Bull. London Math. Soc., **41** (2009), 841–852.

[17] C. J. Mitchell, *An infinite family of symmetric designs,* Discrete Math., **26** (1979), 247–250.

[18] E. T. Parker, *On collineations of symmetric designs,* Proc. Amer. Math. Soc., **8** (1957), 350–351.

[19] P. Ribenboim, "My Numbers, My Friends," Springer-Verlag, New York, 2000.

[20] S. Vajda, "Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications," Ellis Horwood Series: Mathematics and its Applications, Ellis Horwood Ltd., Chichester, 1989.

[21] D. D. Wall, *Fibonacci series modulo m,* Amer. Math. Monthly, **67** (1960), 525–532.

[22] H. N. Ward, *Design lines,* preprint, arXiv:1002.2955v1 [math.CO].