Mathematika 65 (2019) 488–499 © 2019 University College London
doi:10.1112/S0025579318000566

HADAMARD MATRICES AND 1-FACTORIZATIONS OF COMPLETE GRAPHS

KEITH BALL, OSCAR ORTEGA-MORENO AND MARIA PRODROMOU

Abstract. We discuss 1-factorizations of complete graphs that "match" a given Hadamard matrix. We prove the existence of these factorizations for two families of Hadamard matrices: Walsh matrices and certain Paley matrices.

§0. *Introduction.* A 1-factor of a graph G (of even order) is a set of independent edges spanning the vertices of G. A 1-factorization of G is a partition of the set of edges of G into 1-factors.

Given a complete graph with an even number of vertices, it is not difficult to show that there exists a 1-factorization. Let n be an even integer and consider the complete graph K^n. To find a factorization of K^n into 1-factors, select $n-1$ vertices and place them on the vertices of an $(n-1)$-regular $(n-1)$-gon, and place the remaining vertex at the centre of the polygon. To get the first 1-factor, pick any vertex of the polygon and select the edge joining it to the vertex at the centre. For the remaining vertices, select the edges that are perpendicular to the line passing through the centre and the vertex already joined to it. For the remaining 1-factors, just select the $n-2$ clockwise rotations of the first factor (see Figure 1).

However, for the factorizations that we will consider, there will be restrictions on which edges can be selected for each factor. These restrictions will be defined in terms of the rows of a Hadamard matrix. A Hadamard matrix is a matrix with orthogonal rows (and orthogonal columns) whose entries are 1 or -1. Thus, if H is a Hadamard matrix of order n, then $h_{ij} \in \{1, -1\}$ and

$$HH^* = nI_n,$$

where I_n is the identity matrix of order n. It is easy to check that if $n > 2$ a Hadamard matrix can only exist if n is a multiple of 4. We will consider Hadamard matrices for which the first row consists of a vector all of whose entries are 1. Note that for any Hadamard matrix, it is always possible to transform this matrix to a matrix with the first row as desired by multiplying each column by the corresponding sign. We adopt this as the normalized version

Received 25 April 2018, published online 11 February 2019.
MSC (2010): 05B20, 05C70, 11T99 (primary).
Oscar Ortega-Moreno was supported by the Mexican National Council of Science and Technology (CONACYT) grant #579817.

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

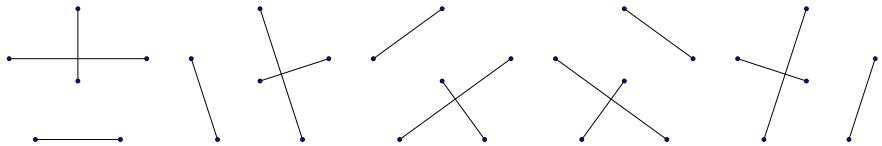


Figure 1: 1-factorization of K^6.

of a given Hadamard matrix. Hence, we will always assume that H is of the form

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \hline \pm 1 & \pm 1 & \cdots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ \pm 1 & \pm 1 & \cdots & \pm 1 \end{pmatrix}.$$

In order to simplify our notation, we make the convention that the indices of the rows of a Hadamard matrix start from 0, so that the second row is $(h_{11}, h_{12}, \ldots, h_{1n})$ and subsequently up to the nth row $(h_{(n-1)1}, h_{(n-1)2}, \ldots, h_{(n-1)n})$:

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \hline h_{11} & h_{12} & \cdots & h_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{(n-1)1} & h_{(n-1)2} & \cdots & h_{(n-1)n} \end{pmatrix}.$$

Given a Hadamard matrix H, we want to find a 1-factorization $\{F_1, F_2, \ldots, F_{n-1}\}$ of K^n such that either each factor satisfies the restriction $R1$ below or each factor satisfies the restriction $R2$ below.

(R1) If an edge e belongs to the factor F_k, then the vertices incident to that edge must have the *opposite* sign in the row k:

$$e = \{i, j\} \in F_k \implies h_{ki}h_{kj} < 0.$$

(R2) If an edge e belongs to the factor F_k, then the vertices incident to that edge must have the *same* sign in the row k:

$$e = \{i, j\} \in F_k \implies h_{ki}h_{kj} > 0.$$

Let us illustrate the problem of finding a factorization satisfying restriction (R1) for the following example:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

We want to find a 1-factorization $\{F_1, F_2, F_3\}$ of the complete graph on four vertices K^4 satisfying restriction (R1). For the row $(1, -1, 1, -1)$, there are four

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

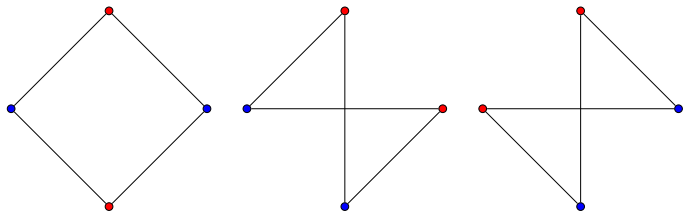


Figure 2: Possible edges we could potentially select for the first, second and third rows of the Hadamard matrix H.

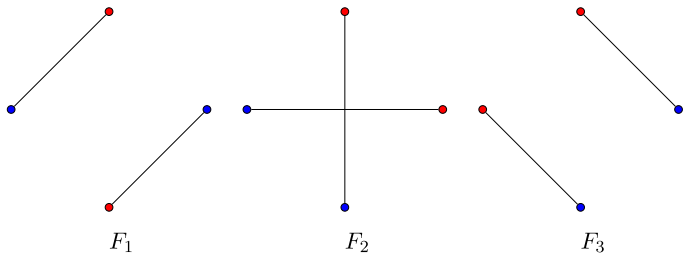


Figure 3: A feasible 1-factorization of K^4 satisfying restriction (R1).

edges we could potentially select; $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$ and $\{1, 4\}$ (see Figure 2). However, the only factors satisfying restriction (R1) are $\{\{1, 2\}, \{3, 4\}\}$ and $\{\{1, 4\}, \{2, 3\}\}$. We do the same analysis for the third row and we see that the only two possible factors are $\{\{1, 3\}, \{2, 4\}\}$ and $\{\{2, 4\}, \{1, 3\}\}$. Finally, for the fourth row we see that the only possible choices are $\{\{1, 3\}, \{2, 4\}\}$ and $\{\{1, 2\}, \{3, 4\}\}$ (see Figure 3).

Hence, from the eight possible combinations of these pairs of edges a feasible 1-factorization of K^4 satisfying the requirements is

$$\begin{aligned} F_1 &= \{\{1, 4\}, \{2, 3\}\}, \\ F_2 &= \{\{1, 3\}, \{2, 4\}\}, \\ F_3 &= \{\{1, 2\}, \{3, 4\}\}. \end{aligned}$$

For the general case of an arbitrary Hadamard matrix the problem seems to be far more complex than for the simple example: however, we conjecture that it is always possible to find 1-factorizations satisfying the two different restrictions.

We can regard the problem as an integer programme. We have a variable $x_{k,\{i,j\}}$ for each row k and pair of columns $\{i, j\}$. We want the variable to be either one or zero according as the edge $\{i, j\}$ belongs to the factor F_k. Hence, in the (R1) case, we want to find integer values $x_{k,\{i,j\}}$ such that

$$0 \leqslant x_{k,\{i,j\}} \leqslant \begin{cases} 0 & \text{if } h_{ki} = h_{kj}, \\ 1 & \text{if } h_{ki} \neq h_{kj} \end{cases} \tag{0.1}$$

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

and, for each edge $\{i, j\}$ in the complete graph K^n,

$$\sum_{k=1}^{n-1} x_{k,\{i,j\}} = 1 \tag{0.2}$$

and, for each $k \in \{1, \ldots, n-1\}$ and $j \in \{1, \ldots, n\}$,

$$\sum_{i \neq j}^{n} x_{k,\{i,j\}} = 1. \tag{0.3}$$

If instead of (0.1) we ask the variables to satisfy

$$0 \leqslant x_{k,\{i,j\}} \leqslant \begin{cases} 0 & \text{if } h_{ki} \neq h_{kj}, \\ 1 & \text{if } h_{ki} = h_{kj}, \end{cases} \tag{0.4}$$

then the solution to the integer programme will be equivalent to finding a 1-factorization satisfying restriction (R2).

The linear relaxation of the integer programme is easily seen to be feasible and the Hadamard condition is just what is needed. Choose

$$x_{k,\{i,j\}} = \begin{cases} \dfrac{2}{n} & \text{if } h_{ki} \neq h_{kj}, \\ 0 & \text{if } h_{ki} = h_{kj}. \end{cases}$$

Since each row of H is orthogonal to the first row, for each k, i there are $n/2$ values of j such that the entries of the row k at the ith and jth columns have opposite sign and therefore $x_{k,\{i,j\}} = 2/n$ for exactly $n/2$ values of j. Thus, restriction (0.3) is satisfied.

On the other hand, each pair of columns of H is orthogonal. Hence, for each $\{i, j\}$ there are $n/2$ rows below the first one for which the entries in the ith and jth columns have opposite sign and therefore again $x_{k,\{i,j\}} = 2/n$ for exactly $n/2$ values of k. Thus, restriction (0.2) is satisfied.

For the same-sign case (restriction (R2)), we choose

$$x_{k,\{i,j\}} = \begin{cases} \dfrac{1}{n/2-1} & \text{if } h_{ki} = h_{kj}, \\ 0 & \text{if } h_{ki} \neq h_{kj}. \end{cases}$$

In the two remaining sections of the paper we solve the 1-factorization problems for two families of Hadamard matrices: Walsh matrices in §1 and certain Paley matrices in §2.

§1. *Factorizations for Walsh matrices.* The Walsh matrices are constructed via an inductive process originally due to Sylvester. Given a Hadamard matrix

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

H of order n, we can construct a new Hadamard matrix of order $2n$ by defining the following matrix by blocks:

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}.$$

Hence, we define

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and we define inductively

$$H_m = \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}$$

for each integer $m > 1$.

THEOREM 1.1. *Let $m > 1$ be an integer and $n = 2^m$. There exist 1-factorizations of K^n satisfying restrictions (R1) and (R2), respectively.*

Proof. The proof is by induction. We want to show first that there are such 1-factorizations for H_2:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

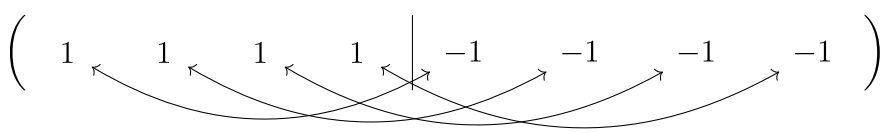
We already saw that there is a factorization satisfying restriction (R1) in our example. On the other hand, it is easy to see that there is one and only one possible choice for a factorization satisfying restriction (R2).

Our inductive hypothesis states that there exist such factorizations satisfying (R1) and (R2) for H_{m-1}. As is common in this kind of induction, we need both types of factorization for H_{m-1} to obtain each factorization of H_m but there is a strange additional issue to consider in one case.

Now

$$H_m = \left(\begin{array}{c|c} H_{m-1} & H_{m-1} \\ \hline H_{m-1} & -H_{m-1} \end{array}\right).$$

To find a factorization for H_m satisfying (R1), we decompose each of the H_{m-1} blocks in the top 2^{m-1} rows selecting edges of opposite sign. For the bottom 2^{m-1} rows we do as follows. The $(2^{m-1}+1)$th row consists of a block of 2^{m-1} positive entries and then a block of 2^{m-1} negative entries. We select the edges $\{i, i+2^{m-1}\}$ for all $i \in \{1, \ldots, 2^{m-1}\}$ (see Figure 4).



https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

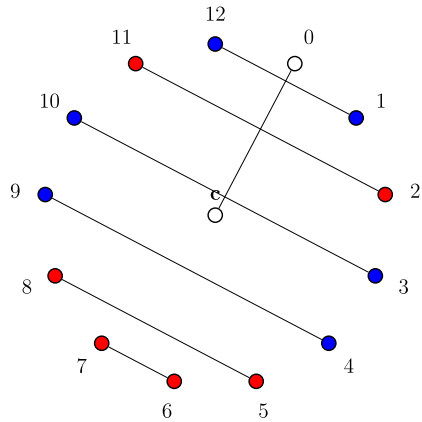


Figure 4: Joining quadratic residues to quadratic residues and non-quadratic residues to non-quadratic residues for $p = 13$.

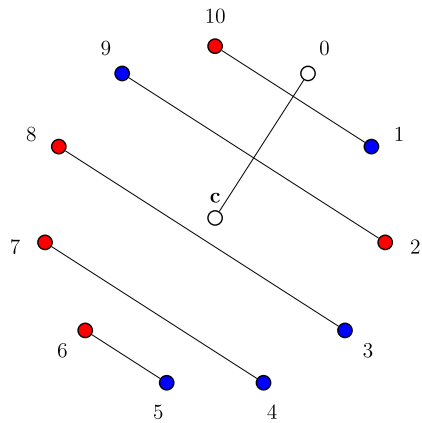
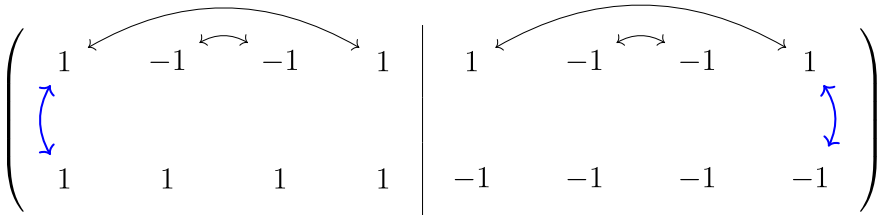


Figure 5: Joining quadratic residues to non-quadratic residues for $p = 11$.

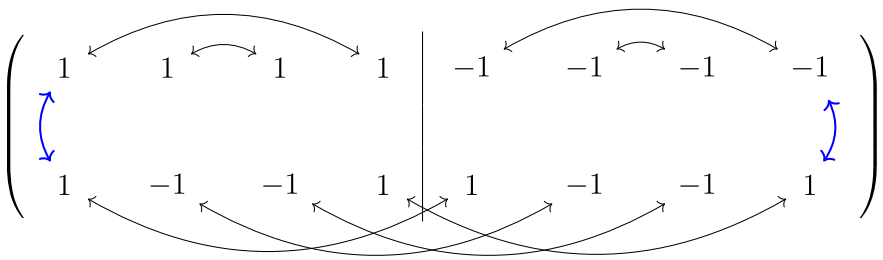
For the remaining rows, using our inductive hypothesis, we select edges of the form $\{i, j + 2^{m-1}\}$ where the pair $\{i, j\}$ appears in a factorization of H_{m-1} satisfying restriction (R2). This gives us a factorization of H_m satisfying restriction (R1).

To find a factorization of H_m satisfying restriction (R2), we decompose each of the H_{m-1} blocks in the top 2^{m-1} rows selecting edges of the same sign. For the bottom 2^{m-1} rows we do as follows. The $(2^{m-1}+1)$th row consists of a block of 2^{m-1} positive entries and then a block of 2^{m-1} negative entries. We swap this row with any of the rows above, let us say the row 2^{m-1} (see Figure 5), choosing the same edges on our new row 2^{m-1} that we already selected in the old row 2^{m-1}.

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press



To select edges in our new $(2^{m-1}+1)$th row, we select edges of the form $\{i, i+2^{m-1}\}$ which have the same sign since they come from the same entry in the matrix H_{m-1}.



For the remaining rows, we select edges of the form $\{i, j+2^{m-1}\}$ where the pair $\{i, j\}$ appears in a factorization of H_{m-1} satisfying restriction (R1). This gives us a factorization of H_m satisfying restriction (R2). □

We are grateful to the referee for pointing out that the method used in the proof of Theorem 1.1 can easily be generalized. The proof shows that for $n \geqslant 2$, if there are 1-factorizations of H_n satisfying (R1) and (R2) respectively then there are 1-factorizations of $H_n \otimes H_1$ satisfying (R1) and (R2). A generalization of this argument can be used to show that for any $m < n$, if there are 1-factorizations of H_n and H_m satisfying (R1) and (R2), then there are 1-factorizations of $H_n \otimes H_m$ satisfying (R1) and (R2).

§2. *Factorizations and the finite field* $\mathbb{Z}_p$. In this section we find 1-factorizations of the complete graph with restrictions defined in terms of matrices constructed using finite fields $\mathbb{Z}_p$, where p is a prime. This construction is due to Paley and we refer the reader to Paley's article for a more detailed explanation of the construction [**2**]. We shall use a very slight variation of the usual Paley matrices. We first set

$$M = \left(\left(\frac{j-i}{p}\right)\right)_{i,j\in\mathbb{Z}_p},$$

where $\left(\frac{k}{p}\right)$ is the Legendre symbol. When $p \equiv 3 \pmod 4$, the Paley matrix H_p is defined to be

$$H_p = \begin{pmatrix} 0 & e \\ -e^T & M \end{pmatrix} + I,$$

where $e = (1, 1, \ldots, 1) \in \mathbb{R}^p$ and I is the identity matrix of order $p+1$.

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

The main theorem of this section is the following, in which a "near-primitive root" modulo p is just the square of a primitive root.

THEOREM 2.1. *Let p be a prime such that $p \equiv 3 \pmod 4$; then we can find a 1-factorization of the complete graph K^{p+1} satisfying restriction (R1) with respect to the Paley matrix of order $p+1$.*

If in addition we assume that 2 is a near-primitive root modulo p, then we can find a 1-factorization of the complete graph K^{p+1} satisfying restriction (R2).

It is natural to try to prove this theorem in the following way. Since the rows of M are just cyclic permutations of the first row, it seems reasonable to find a 1-factor corresponding to the second row of H_p and then cycle it to obtain 1-factors for the other rows just as in the example at the start of the article. This will work provided our 1-factor contains, within the matrix M, exactly one edge $\{i, j\}$ of each possible length: $i - j = \pm 1, \pm 2, \ldots, \pm(p-1)/2$. So, we are led to consider the following problem, which makes sense regardless of whether p is congruent to 1 or 3 modulo 4.

Problem 2.2. Let p be any prime number and K^{p+1} the complete graph with vertex set $\mathbb{Z}_p \cup \{\mathbf{c}\}$, where $\mathbf{c}$ is an additional point that we will call the centre. We adopt the convention that the length of any edge containing the centre is infinity, that the vertex 0 is a residue and that the centre $\mathbf{c}$ is a non-residue.

(P1) Is there a 1-factor of K^{p+1} such that each edge selected is either incident to two quadratic residues or incident to two non-residues, and such that the lengths of the edges are all different from one another?

(P2) Is there a 1-factor of K^{p+1} such that each edge selected is incident to a quadratic residue and a non-residue, and such that the lengths of the edges are all different from one another?

There are two easy cases. The first one is when $p \equiv 1 \pmod 4$ and we want to join quadratic residues to quadratic residues, and non-quadratic residues to non-quadratic residues. The second one is when $p \equiv 3 \pmod 4$ and we want to join residues to non-residues. These two cases are done using the following observation: -1 is a quadratic residue if and only if $p \equiv 1 \pmod 4$. Hence, when $p \equiv 1 \pmod 4$, we can select the edges of the form $\{r, -r\}$ where $r \in \{1, \ldots, (p-1)/2\}$ and, by our previous observation, r and $-r$ are either both quadratic residues or both non-quadratic residues. The length of the edge $\{r, -r\}$ is $2r$ and all these lengths are clearly different from one another for $r \in \{1, \ldots, (p-1)/2\}$. We do exactly the same selection of edges when $p \equiv 3 \pmod 4$ but in this case we now join quadratic residue to non-quadratic residues by our observation.

Hence, we have the following theorems.

THEOREM 2.3. *Let p be a prime such that $p \equiv 1 \pmod 4$; then there exists a 1-factor of the complete graph with vertex set $\mathbb{Z}_p \cup \{c\}$ consisting of edges of all possible lengths matching residues to residues, and non-residues to non-residues.*

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

THEOREM 2.4. *Let p be a prime such that $p \equiv 3 \pmod 4$; then there exists a 1-factor of the complete graph with vertex set $\mathbb{Z}_p \cup \{c\}$ consisting of edges of all possible lengths matching residues to non-residues.*

We now turn to the difficult cases. First, let p be a prime such that $p \equiv 1 \pmod 4$. In this case, we want to join residues to non-residues. Let x be a primitive root modulo p. We shall consider edges of the form $e_k = \{x^k, x^{k+1}\}$, where $k = 0, \ldots, p-1$. Each of these edges joins a residue to a non-residue. The length of the edge is $x^{k+1} - x^k = x^k(x-1)$. These numbers are all different as k runs from 0 to $p-1$ but we wish to exclude the possibility that the edges that we choose include an opposite pair $\pm y$. The edges e_j and e_k have opposite lengths if

$$x^{k-j} = -1 = x^{(p-1)/2}.$$

Our aim will be to select $(p-3)/2$ which are different from one another and their negatives. These will join $p-3$ elements of $\mathbb{Z}_p^*$ and we wish to leave unjoined two elements: a residue r that we shall connect to 0 and a non-residue n that we shall connect to the centre.

We therefore need to ensure that $\pm r$ is not one of the lengths that we have selected. Now if $r = x^k$ then we will not use the edge $\{x^k, x^{k+1}\}$ whose length is $x^k(x-1) = r(x-1)$ and this will indeed be r provided $x = 2$. Henceforth, we assume this to be the case (which necessarily means that $p \equiv 5 \pmod 8$). It then does not matter which residue we choose for r, so we take $r = 1 = 2^0$ and $n = -2 = 2^{(p+1)/2}$. We have used the vertex $r = 1$ and the length 1. We select the remaining edges to be

$$\begin{aligned} e_1 &= \{2, 4\} = \{2^1, 2^2\}, \\ e_3 &= \{8, 16\} = \{2^3, 2^4\}, \\ &\vdots \\ e_{(p-3)/2} &= \{2^{(p-3)/2}, -1\} = \{2^{(p-3)/2}, 2^{(p-1)/2}\} \end{aligned}$$

and

$$\begin{aligned} e_{(p+3)/2} &= \{-4, -8\} = \{2^{(p+3)/2}, 2^{(p+5)/2}\}, \\ e_{(p+7)/2} &= \{-16, -32\} = \{2^{(p+7)/2}, 2^{(p+9)/2}\}, \\ &\vdots \\ e_{p-3} &= \{2^{p-3}, 2^{p-2}\}. \end{aligned}$$

By inspection (see Figure 6), we see that the lengths of the edges that we have selected are not equal nor equal to their negatives and we have not used the edges of length ± 1, which are e_0 and e_{p-2}. We are thus at liberty to join 1 to 0.

The second difficult case is that of a prime $p \equiv 3 \pmod 4$ and we want to join quadratic residues to quadratic residues and non-residues to non-residues. In this case we will assume that there a primitive root x modulo p such that $x^2 = 2$

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

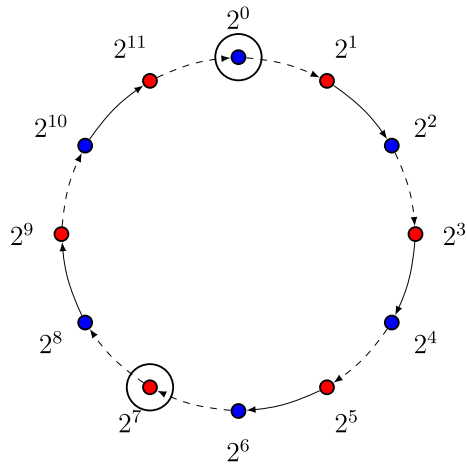


Figure 6: The figure shows the Cayley graph associated with $\mathbb{Z}_p^*$ for the generator 2 and the selection of edges for the case $p = 13$. The edges we select for the perfect matching are the solid lines joining quadratic residues to non-residues.

(which necessarily implies that $p \equiv 7 \pmod 8$). Since $p \equiv 3 \pmod 4$, we know that -1 is not a quadratic residue.

We shall consider edges of the form $e_{2k} = \{x^{2k}, x^{2(k+1)}\}$ which join quadratic residues and edges of the form $e_{2k+(p-1)/2} = \{-x^{2k}, -x^{2(k+1)}\} = \{x^{2k+(p-1)/2}, x^{2(k+1)+(p-1)/2}\}$ which join non-residues. The length of e_k is $x^{2(k+1)} - x^{2k} = x^{2k}(x^2 - 1) = x^{2k}$ and the length of $e_{2k+(p-1)/2}$ is $-x^{2k}$. These lengths are all different as k goes from 0 to $(p-3)/2$ since the negative of the length of e_{2k} is equal to the length of $e_{2k+(p-1)/2}$. The lengths of edges joining quadratic residues to quadratic residues are all different from one another and their negatives and the same is true for the edges joining non-residues to non-residues.

Our aim is to select $(p-3)/2$ which are different from one another and their negatives. These will join $p-3$ elements of $\mathbb{Z}_p^*$ and we wish to leave two elements alone: a quadratic residue r which we shall connect to 0 and a non-residue n which we shall connect to the center $\mathbf{c}$.

We need to ensure that $\pm r$ is not one of the lengths that we have selected. We again take $r = 1$ and $n = -x^{p+3} = x^{2+(p-1)/2} = -2$. We select the remaining edges to be

$$\begin{aligned} e_2 &= \{2, 4\} = \{x^2, x^4\}, \\ e_6 &= \{8, 16\} = \{x^6, x^8\}, \\ &\vdots \\ e_{p-5} &= \{x^{p-5}, x^{p-3}\} \end{aligned}$$

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

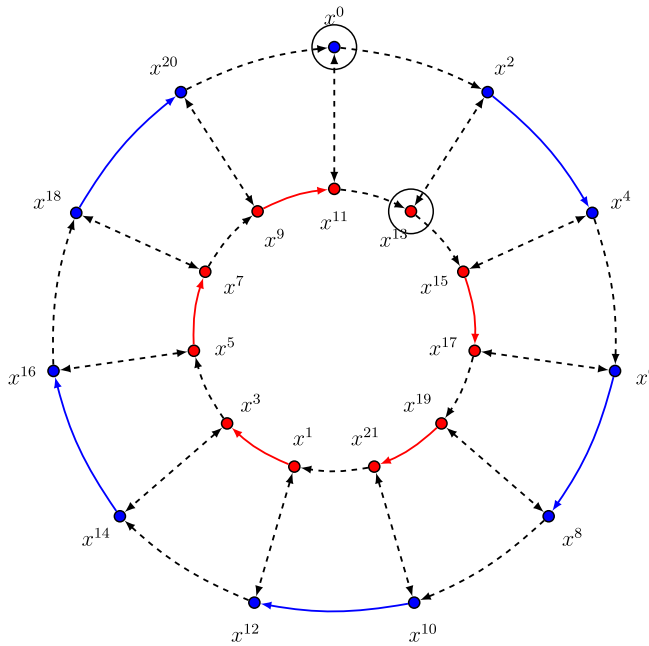


Figure 7: (Colour online) The figure shows the Cayley graph associated with $\mathbb{Z}_p^*$ for the generating set $\{x^2, x^{(p-1)/2}\} = \{2, -1\}$ and the selection of edges incident to either two quadratic residues or two non-residues, in solid blue and red lines, respectively, for the case $p = 23$.

and

$$\begin{aligned} e_{(p-1)/2+4} &= \{-x^4, -x^6\}, \\ e_{(p-1)/2+8} &= \{-x^8, -x^{10}\}, \\ &\vdots \\ e_{(p-1)/2+p-3} &= \{-x^{p-3}, -x^{p-1}\}. \end{aligned}$$

By inspection (see Figure 7), we see that the lengths of the edges that we have selected are not equal or equal to their negatives and we have not used the edges of length ± 1, which are e_0 and $e_{(p-1)/2}$.

To sum up, we have the following theorems.

THEOREM 2.5. *Let p be a prime such that $p \equiv 1 \pmod 4$ and 2 is a primitive root modulo p. Then there exists a 1-factor of the complete graph with vertex set $\mathbb{Z}_p \cup \{c\}$ consisting of edges of all possible lengths matching residues to non-residues.*

THEOREM 2.6. *Let p be a prime such that $p \equiv 3 \pmod 4$ and 2 is a near-primitive root of p. Then there exists a perfect matching of the complete graph*

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press

with vertex set $\mathbb{Z}_p \cup \{c\}$ consisting of edges of all possible lengths matching residues to residues, and non-residues to non-residues.

Even though the proofs of Theorems 2.5 and 2.6 required an additional assumption on p (concerning the number 2), we believe that they should be true in general. Theorem 2.5 is stated for primes p of the form $8k+5$ for which 2 is a primitive root modulus p. It was pointed out to us by Peter Moree that under the generalized Riemann hypothesis there are infinitely many primes of this form and that these have a natural density which is a rational multiple of the Artin constant. This is an example of a generalization of Artin's conjecture asking for the density of primes p in an arithmetic progression such that an integer x is a primitive root modulo p. This was first found by Moree in his article [**1**].

On the other hand, Theorem 2.6 is stated for primes of the form $8k+7$ for which there is a primitive root x modulo p such that $x^2 = 2$. In this case the question is whether there are infinitely many primes in an arithmetic progression for which a given integer t is a near-primitive root. It was pointed out to us by Moree that this situation has not been worked out in the literature but that in our specific situation it would require no new ideas to do it.

To finish, we remark that Problem 2.2 has a natural generalization.

Problem 2.7. Let $A \cup B$ be a partition of the cyclic group C_n, where n is odd. Is it always possible to find a set of $(n-1)/2$ edges $\{x, y\}$ with $x, y \in C_n$, whose $n-1$ lengths $\pm(x-y)$ include each non-zero element of C_n exactly once and so that each edge joins either two elements of A or two of B.

We do not know of any counterexample to this problem: indeed we know of no counterexample even if we replace C_n with any finite group of odd order.

References

1. P. Moree, On primes in arithmetic progression having a prescribed primitive root. *J. Number Theory* **78**(1) (1999), 85–98.
2. R. E. Paley, On orthogonal matrices. *Stud. Appl. Math.* **12**(1–4) (1933), 311–320.

Keith Ball,
Mathematics Institute,
Zeeman Building,
University of Warwick,
Coventry CV4 7AL,
U.K.
E-mail: kmb120205@googlemail.com

Oscar Ortega-Moreno,
Mathematics Institute,
Zeeman Building,
University of Warwick,
Coventry CV4 7AL,
U.K.
E-mail: o.a.ortega-moreno@warwick.ac.uk

Maria Prodromou,
Mathematics Department,
Westminster Academy,
The Naim Dangoor Centre,
255 Harrow Road,
London W2 5EZ,
U.K.
E-mail: m.n.prodromou@gmail.com

https://doi.org/10.1112/S0025579318000566 Published online by Cambridge University Press