# 2. A FAMILY OF (p – 1)-modular circulant Hadamard matrices of size 4p.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **47 (2001)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

Even though the constraints for type 2 seem to be much stronger than the one for type 1, this may not necessarily be so. Consider, for example, the case of size $n = 20$ and modulus $m = 16$. Let

$$X = (1,1,1,-1,1,-1,-1,-1,-1,1,1,-1,-1,1,-1,1,1,1,1,-1).$$

Then, quite surprisingly perhaps, circ($X$) is a 16-modular CHM of type 2, as $X$ satisfies the equalities $\gamma_k(X) = 0$ for all $k \neq 0, 10$, and $\gamma_{10}(X) = -16$.

However, it follows from formula (1) above that there is no 16-modular CHM of type 1 in size 20. Indeed, for $n = 20$, substituting $z = 1$ in formula (1) with $\gamma_{10} = 0$ yields $H(1)^2 = 20 + 2\sum_{k=1}^{9}\gamma_k$.

The condition $\gamma_k \equiv 0 \mod 16$ for $k = 1, \dots, 9$ would imply $(H(1)/2)^2 \equiv 5 \mod 8$, contradicting the fact that 5 is not a square modulo 8. Hence, the condition $\gamma_{10}(X) = 0$ alone forbids the other correlation coefficients of $X$, at positive indices $k$, to vanish simultaneously modulo 16.

The same argument shows that for $q$ odd with $q \not\equiv 1 \mod 8$, there is no 16-modular CHM of length $4q$ satisfying $\gamma_{2q} \equiv 0 \mod 32$.

In this note, we exhibit (in the next section) a 4-parameter family of $(p-1)$-modular circulant Hadamard matrices of type 1 and of size $4p$ for every prime number $p$ such that $p \equiv 1 \mod 4$.

As to circulant modular Hadamard matrices of type 2, it turns out that they can be obtained from a well known paper of Delsarte, Goethals and Seidel [DGS]. This is explained in Section 3.

## 2. A FAMILY OF $(p-1)$-MODULAR CIRCULANT HADAMARD MATRICES OF SIZE $4p$.

Let $p$ be a *prime* satisfying $p \equiv 1 \mod 4$. We are going to prove the existence of $(p-1)$-modular circulant Hadamard matrices of type 1 and size $4p$. We give explicitly below the first row $(x_0, x_1, \dots, x_{4p-1})$ of such a matrix as a polynomial $H(z) = \sum_{i=0}^{4p-1} x_i z^i \in \mathbf{Z}C_{4p} = \mathbf{Z}[z]/(z^{4p}-1)$, where all coefficients $x_i$ equal $\pm 1$ and $H(z)H(z^{-1}) \equiv 4p$ modulo $(p-1)\mathbf{Z}C_{4p}$. In order to write down $H(z)$ we need some notation.

Let $S_0 \subset [1, p-1] \cup [p+1, 2p-1]$ be the set of squares modulo $2p$, which are prime to $p$. Note that if $s$ is a square mod $p$, then $s$ is also a square mod $2p$. Indeed, if there exists $c$ such that $c^2 = s + kp$ and $k$ is odd, then $(c+p)^2 = c^2 + 2cp + p^2 = s + 2cp + (k+p)p \equiv s \mod 2p$.

Let $S_1 = ([1,p-1] \cup [p+1,2p-1]) \backslash S_0$ be the set of non-squares mod $2p$, prime to $p$. We have $|S_0 \cap [1,p-1]| = |S_0 \cap [p+1,2p-1]| = \frac{p-1}{2}$, so that $|S_0| = p-1$. Similarly, $|S_1 \cap [1,p-1]| = |S_1 \cap [p+1,2p-1]| = \frac{p-1}{2}$ and $|S_1| = p-1$ also.

Let $f_0(z)$ and $f_1(z)$ be the Hall polynomials of $S_0$ and $S_1$ respectively. That is, $f_i(z) = \sum_{s \in S_i} z^s \in \mathbf{Z}C_{4p}$ for $i = 0, 1$. We shall need $f_i(z^2) = \sum_{s \in S_i} z^{2s}$ and $f_i(-z^2) = \sum_{s \in S_i} (-1)^s z^{2s}$. Our objective is the proof of the following theorem.

THEOREM 1. *Let $f_0$ and $f_1$ be as defined above and let $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3$ be 4 independent parameters with values $\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3 = \pm 1$. The polynomial $H(z) \in \mathbf{Z}C_{4p} = \mathbf{Z}[z]/(z^{4p}-1)$ given by*

$$H(z) = \varepsilon_0\big(1 + f_0(z^2) + z^{2p}\big) + \varepsilon_1 f_0(z^2)\, z^p + \varepsilon_2 f_1(-z^2) + \varepsilon_3\big(1 + f_1(-z^2) - z^{2p}\big)\, z^p$$

*has all its coefficients of the monomials $1, z, z^2, \ldots, z^{4p-1}$ equal to $\pm 1$ and satisfies the identity*

$$H(z)H(z^{-1}) = 4p + (p-1)R(z)$$

*for some polynomial $R(z) \in \mathbf{Z}[z]/(z^{4p}-1)$ given below in formula* (11) *in which the coefficient of $z^{2p}$ is zero.*

The exponents of $z$ in $H$ and $R$ are to be read modulo $4p$. We use (abusively) the term "polynomial" for the elements of $\mathbf{Z}[z]/(z^{4p}-1)$. The assertion on the coefficients of $H$ is easy to verify by direct observation and is left to the reader.

The parameter $\varepsilon_0$ is clearly the coefficient of the constant term in the displayed expression for $H(z)$. The coefficient of $z$ in $H(z)$ is $\varepsilon_1$ on the condition that $p \equiv 1 \mod 8$. Indeed, in this case 2 is a square mod $p$. Also $3p+1$ is a square mod $2p$ and therefore $\frac{3p+1}{2} \in S_0$. Thus, the term $z = z^{2\frac{3p+1}{2}+p}$ appears in $\varepsilon_1 f_0(z^2) z^p$. If $p \equiv 5 \mod 8$, then $\frac{3p+1}{2} \in S_1$ and $z$ appears in $H(z)$ with the coefficient $(-1)^{\frac{3p+1}{2}} \varepsilon_3 = +\varepsilon_3$. The first appearance of $\varepsilon_2$ in $H(z)$ depends on the minimum of $S_1$, a number for which there is no known formula.

For the proof of the theorem we separate a preliminary part, which only depends on symmetry properties of the set $S_0$, from the final calculation, which properly depends on the hypothesis that $S_0$ is constructed from the set of quadratic residues mod $p$.

We first derive the properties of $H(z)H(z^{-1})$ coming from the symmetries of the set $S_0$ and its complement $S_1 = ([1,p-1] \cup [p+1,2p-1]) \backslash S_0$. We denote by $\varphi\colon [1,p-1] \cup [p+1,2p-1] \to [1,p-1] \cup [p+1,2p-1]$ the flip defined by the formula $\varphi(x) = 2p - x$.

Whenever the set $S_0$ is stable under $\varphi$, the existence of $\varphi\colon S_0 \to S_0$, and hence $\varphi\colon S_1 \to S_1$, implies the following properties of the sums $\sum_{s\in S_i} z^{2s}$ as well as $\sum_{s\in S_i}(-1)^s z^{2s}$ for the sets $S_i$ with $i = 0, 1$:

$$\sum_{s\in S_i} z^{-2s} = \sum_{s\in S_i} z^{2s}, \qquad \sum_{s\in S_i}(-1)^s z^{-2s} = \sum_{s\in S_i}(-1)^s z^{2s}. \tag{2}$$

This follows simply by applying the involution $\varphi$.

For instance,

$$\begin{aligned}\sum_{s\in S_i}(-1)^s z^{2s} &= \sum_{s\in S_i}(-1)^{\varphi(s)} z^{2\varphi(s)}\\ &= \sum_{s\in S_i}(-1)^{(2p-s)} z^{2(2p-s)}\\ &= \sum_{s\in S_i}(-1)^s z^{-2s},\end{aligned}$$

since $z^{4p} = 1$. This means that $f_0(-z^2)$ and $f_1(-z^2)$ are both self-reciprocal polynomials: $f_0(-z^2) = f_0(-z^{-2})$ and $f_1(-z^2) = f_1(-z^{-2})$. The proof for the other formula (without the sign) is essentially the same.

We also have a "baker's flip" $\rho$, mapping $[1,p-1] \cup [p+1,2p-1]$ onto itself, defined by

$$\rho(x) = \begin{cases} p - x & \text{if } x \in [1,p-1],\\ 3p - x & \text{if } x \in [p+1,2p-1].\end{cases}$$

If $S_0$ and $S_1$ are stable under $\rho$, the existence of the automorphisms $\rho\colon S_i \to S_i$ for $i = 0, 1$ implies the following formulas:

$$(1 - z^{2p}) \sum_{s\in S_i} z^{2s} = 0, \qquad (1 + z^{2p}) \sum_{s\in S_i}(-1)^s z^{2s} = 0. \tag{3}$$

Here we apply $\rho$ on $S_i \cap [1,p-1]$, and on $S_i \cap [p+1,2p-1]$. We have

$$\begin{aligned}\sum_{s\in S_i}(-1)^s z^{2s} &= \sum_{s\in S_i}(-1)^{\rho(s)} z^{2\rho(s)}\\ &= \sum_{s\in S_i\cap[1,p-1]}(-1)^{p-s} z^{2(p-s)} + \sum_{s\in S_i\cap[p+1,2p-1]}(-1)^{3p-s} z^{2(3p-s)}.\end{aligned}$$

Remembering that $z^{4p} = 1$, we obtain

$$\begin{aligned}\sum_{s\in S_i}(-1)^s z^{2s} &= -z^{2p}\sum_{s\in S_i}(-1)^s z^{-2s}\\ &= -z^{2p}\sum_{s\in S_i}(-1)^{(2p-s)} z^{2(2p-s)}\\ &= -z^{2p}\sum_{s\in S_i}(-1)^s z^{2s},\end{aligned}$$

using the automorphism $\varphi$ as above. Again, the proof for the formula without the sign is the same.

As a corollary, we get

$$f_i(-z^2)f_j(z^2) = \Big(\sum_{s\in S_i}(-1)^s z^{2s}\Big)\Big(\sum_{t\in S_j} z^{2t}\Big) = 0\,, \tag{4}$$

obtained by observing that $(1+z^{2p})$ and $(1-z^{2p})$ both kill the above product. The first factor is killed by $1+z^{2p}$. The second one by $1-z^{2p}$. It follows that $2 = (1+z^{2p})+(1-z^{2p})$ annihilates the left-hand side of (4), which must be $0$ since $2$ is not a zero-divisor in $\mathbf{Z}C_{4p}$.

We can begin the calculation of some terms in $H(z)H(z^{-1})$. Under the hypothesis $p \equiv 1 \mod 4$ of the theorem, $-1$ is a square mod $p$ and $-1$ is also a square mod $2p$. Therefore, $p-1 \in S_0$ and it follows that $S_0$, $S_1$ are stable by both involutions $\rho$, $\varphi$. The formulas (2), (3) and (4) apply.

As a consequence, we obtain that the coefficients of $\varepsilon_0\varepsilon_2$, $\varepsilon_1\varepsilon_2$, $\varepsilon_0\varepsilon_3$ and $\varepsilon_1\varepsilon_3$ in $H(z)H(z^{-1})$ all vanish. For instance, in the coefficient of $\varepsilon_0\varepsilon_3$ in $H(z)H(z^{-1})$, which is

$$2\Big(1+\big(\sum_{s\in S_0} z^{2s}\big)+z^{2p}\Big)\Big(1+\big(\sum_{s\in S_1}(-1)^s z^{2s}\big)-z^{2p}\Big)(z^p+z^{-p}),$$

the products of $1+z^{2p}$ with $1-z^{2p}$ and $\sum_{s\in S_1}(-1)^s z^{2s}$ are 0. Furthermore, the products of $\sum_{s\in S_0} z^{2s}$ with $1-z^{2p}$ and with $\sum_{s\in S_1}(-1)^s z^{2s}$ also vanish.

The coefficients of the other terms $\varepsilon_0\varepsilon_2$, $\varepsilon_1\varepsilon_2$ and $\varepsilon_1\varepsilon_3$ are seen to be 0 by the same arguments based on formulas (2), (3) and (4). The coefficient of $\varepsilon_2\varepsilon_3$ is

$$(z^p+z^{-p})\Big(\sum_{s\in S_1}(-1)^s z^{2s}\Big)\Big(1+\sum_{s\in S_1}(-1)^s z^{2s}-z^{2p}\Big)\,.$$

Although of a somewhat different nature, it also vanishes by formula (3), observing that $z^p+z^{-p} = z^p(1+z^{2p})$.

The only remaining terms in $H(z)H(z^{-1})$ are

$$H(z)H(z^{-1}) = \left(1+f_0(z^2)+z^{2p}\right)^2 + \left(1+f_1(-z^2)-z^{2p}\right)^2 + \left(f_1(-z^2)\right)^2 + \left(f_0(z^2)\right)^2 + 2\,\varepsilon_0\,\varepsilon_1\left(1+f_0(z^2)+z^{2p}\right)f_0(z^2)(z^p+z^{-p}).$$

We end up with an expression $H(z)H(z^{-1}) = C + C_{0,1}\,\varepsilon_0\,\varepsilon_1$.

An easy calculation using formula (3) and the simple remarks $(1+z^{2p})^2 = 2(1+z^{2p})$, $(1-z^{2p})^2 = 2(1-z^{2p})$, yields

$$C = 2\{(f_0(z^2))^2 + 2f_0(z^2) + (f_1(-z^2))^2 + 2f_1(-z^2)\} + 4,$$

and similarly

$$C_{0,1} = 2\big((f_0(z^2))^2 + 2f_0(z^2)\big)(z^p + z^{-p}),$$

which require the computation of the two squares $(f_0(z^2))^2 = \left(\sum_{s\in S_0} z^{2s}\right)^2$ and $(f_1(-z^2))^2 = \left(\sum_{s\in S_1}(-1)^s z^{2s}\right)^2$.

We shall actually need to calculate all four quantities $(f_0(z^2))^2$, $(f_1(z^2))^2$, $(f_0(-z^2))^2$, $(f_1(-z^2))^2$. For brevity, we use the notation

$$X_i = f_i(z^2) = \sum_{s\in S_i} z^{2s}, \qquad Y_i = f_i(-z^2) = \sum_{s\in S_i}(-1)^s z^{2s},$$

for $i = 0, 1$.

Note first that $X_0 + X_1 = \sum_{\nu=0}^{2p-1} z^{2\nu} - (1+z^{2p}) = T - (1+z^{2p})$, where we have set $T = \sum_{\nu=0}^{2p-1} z^{2\nu}$. Similarly, $Y_0 + Y_1 = \sum_{\nu=0}^{2p-1}(-1)^\nu z^{2\nu} - (1-z^{2p}) = U - (1-z^{2p})$, where $U = \sum_{\nu=0}^{2p-1}(-1)^\nu z^{2\nu}$.

Observe that $z^2T = T$ and $z^2U = -U$. It follows that

$$X_0^2 + 2X_0X_1 + X_1^2 = (T-(1+z^{2p}))^2 = 2(p-2)T + 2(1+z^{2p}). \tag{5}$$

We also have $(X_0 - X_1)T = |S_0|T - |S_1|T = 0$, and thus

$$X_0^2 - X_1^2 = (T-(1+z^{2p}))(X_0-X_1) = -2(X_0-X_1), \tag{6}$$

remembering formula (3).

The main point is the calculation of $(X_0 - X_1)^2$, which is reminiscent of the familiar calculation with Gauss sums.

Let $\left(\frac{\cdot}{p}\right)\colon \mathbf{Z} \to \{\pm 1\}$ be the quadratic character at the prime $p$ extended to the integers as usual: $\left(\frac{x}{p}\right) = 0$ if $x$ is divisible by $p$, $\left(\frac{x}{p}\right) = +1$ if $x$, prime to $p$, is a quadratic residue modulo $p$ (i.e., $x \equiv y^2$ modulo $p$ for some $y$) and $\left(\frac{x}{p}\right) = -1$ if $x$ is prime to $p$ and not a quadratic residue modulo $p$. We are assuming $p \equiv 1 \bmod 4$, and hence $\left(\frac{-1}{p}\right) = 1$.

Notice that $X_0 - X_1 = \sum_{x=0}^{2p-1} \left(\frac{x}{p}\right) z^{2x} = (\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) z^{2x})(1 + z^{2p})$ since $\left(\frac{x+p}{p}\right) = \left(\frac{x}{p}\right)$ for all $x$. For all integers $x, y$ we have $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$ and thus

$$(X_0 - X_1)^2 = 2\Big(\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\tfrac{xy}{p}\right) z^{2(x+y)}\Big)(1 + z^{2p}).$$

Now, observe that $z^{2(t+p)}(1+z^{2p}) = z^{2t}(1+z^{2p})$ for any integer $t$. It follows that, identifying the set of integers $[1, p-1]$ with $\mathbf{F}_p^* = \mathbf{F}_p \backslash \{0\}$ by the natural projection $\mathbf{Z} \to \mathbf{F}_p$, we have

$$(X_0 - X_1)^2 = 2\Big(\sum_{x,y \in \mathbf{F}_p^*} \left(\tfrac{xy}{p}\right) z^{2(x+y)}\Big)(1 + z^{2p}).$$

The crucial point is that the right-hand side is well defined, without ambiguity even though the expression $\sum_{x,y\in\mathbf{F}_p^*} \left(\frac{xy}{p}\right) z^{2(x+y)}$ in itself is only defined modulo $(z^{2p} - 1)$.

For fixed $x \in \mathbf{F}_p^*$, as $y$ runs over $\mathbf{F}_p^*$, so does $-yx$; therefore

$$\begin{aligned}(X_0 - X_1)^2 &= 2\Big(\sum_{x,y \in \mathbf{F}_p^*} \left(\tfrac{-x^2 y}{p}\right) z^{2x(1-y)}\Big)(1 + z^{2p}) \\ &= 2\left(\tfrac{-1}{p}\right)\Big(\sum_{x,y \in \mathbf{F}_p^*} \left(\tfrac{y}{p}\right) z^{2x(1-y)}\Big)(1 + z^{2p}).\end{aligned}$$

Summing over $x$ for $y = 1$ and then for $y \in \mathbf{F}_p^* \backslash \{1\}$, we get

$$(X_0 - X_1)^2 = 2\left(\tfrac{-1}{p}\right)\{(p-1) + \sum_{y \in \mathbf{F}_p^* \backslash \{1\}} \left(\tfrac{y}{p}\right) \sum_{x \in \mathbf{F}_p^*} z^{2x}\}(1 + z^{2p}).$$

Since $\sum_{y\in\mathbf{F}_p^*} \left(\frac{y}{p}\right) = 0$, we have $\sum_{y\in\mathbf{F}_p^*\backslash\{1\}} \left(\frac{y}{p}\right) = -1$. Using $\left(\frac{-1}{p}\right) = +1$, and coming back to a summation over $[1, p-1]$,

$$\begin{aligned}(X_0 - X_1)^2 &= 2\{(p-1) - \sum_{x=1}^{p-1} z^{2x}\}(1 + z^{2p}) \\ &= 2(p-1)(1 + z^{2p}) - 2(T - (1 + z^{2p})) = 2p(1 + z^{2p}) - 2T.\end{aligned}$$

This gives us

$$X_0^2 - 2X_0X_1 + X_1^2 = 2p(1 + z^{2p}) - 2T. \tag{7}$$

Combining this result with the equations (5) and (6), we see that

$$X_0^2 + 2X_0X_1 + X_1^2 = 2(p-2)T + 2(1+z^{2p}),$$
$$X_0^2 - X_1^2 = -2(X_0 - X_1),$$
$$X_0^2 - 2X_0X_1 + X_1^2 = -2T + 2p(1+z^{2p}).$$

It is now easy to deduce from these equations the result:

$$X_0^2 + 2X_0 = X_1^2 + 2X_1 = \tfrac{p-1}{2}(T + 1 + z^{2p}). \tag{8}$$

Of course we would also like to have a similar formula for $Y_0$, $Y_1$. The analogue of equation (5) is

$$Y_0^2 + 2Y_0Y_1 + Y_1^2 = (U - (1-z^{2p}))^2 = 2(p-2)U + 2(1-z^{2p}),$$

on observing that $z^2U = -U$, so that $z^{2s}U = (-1)^sU$ and $U^2 = 2pU$. It is easy, though somewhat boring, to imitate with $Y_0$ and $Y_1$ the derivation of the formulas (5), (6) and (7). The needed assertion, that $\left(\frac{x}{p}\right)(-1)^t z^{2t}(1-z^{2p})$ only depends on the class of $t \bmod p$, is valid and the argument goes through.

The analogue of the above equation (8) is

$$Y_0^2 + 2Y_0 = Y_1^2 + 2Y_1 = \tfrac{p-1}{2}(U + 1 - z^{2p}). \tag{9}$$

However, we can simply embed the ring $\mathbf{Z}C_{4p}$ into $\mathbf{Z}[\mathbf{i}]C_{4p}$, the group ring of $C_{4p}$ over the Gaussian integers $\mathbf{Z}[\mathbf{i}]$, $\mathbf{i} = (\sqrt{-1})$, and then apply to the calculations of $X_0$, $X_1$ the automorphism $\sigma$ of the ring $\mathbf{Z}[\mathbf{i}][z]/(z^{4p}-1)$ induced by $\sigma(z) = (\sqrt{-1})z$. The substitution of $(\sqrt{-1})z$ for $z$ is compatible with $z^{4p} = 1$ and $\sigma(X_i) = Y_i$, $\sigma(T) = U$ and $\sigma(z^{2p}) = -z^{2p}$. The result is indeed formula (9) above.

Using $T+U = 2\sum_{\nu=0}^{p-1} z^{4\nu}$, and plugging these expressions into the formula for $H(z)H(z^{-1}) = C + C_{0,1}\,\varepsilon_0\,\varepsilon_1$, we get

$$C = (q-1)(T+U+2) + 4 = 4p + 2(p-1)\sum_{\nu=1}^{p-1} z^{4\nu}$$

and

$$C_{0,1} = \frac{p-1}{2}(T + (1+z^{2p}))(z^p + z^{-p}) = (p-1)\Big(\sum_{\nu=1}^{2p} z^{2\nu-1}\Big) + (p-1)(z^p + z^{3p}).$$

Finally, $H(z)H(z^{-1}) = 4p + (p-1)R(z)$, where

$$R(z) = 2\sum_{\nu=1}^{p-1} z^{4\nu} + \Big\{\sum_{\nu=1}^{2p} z^{2\nu-1} + z^p + z^{3p}\Big\}\,\varepsilon_0\,\varepsilon_1. \tag{10}$$

Equivalently, this "remainder" $R(z)$ can be written

$$(11)\quad R(z) = 2\sum_{\nu=1}^{\frac{p-1}{2}}(z^{4\nu}+z^{-4\nu}) + \left\{\sum_{\nu=1}^{p}(z^{2\nu-1}+z^{-(2\nu-1)}) + z^p + z^{-p}\right\}\varepsilon_0\,\varepsilon_1\,.$$

The (periodic) correlations of $H(z)$ in degrees $\equiv 2 \mod 4$ are strictly zero. This includes in particular the correlation of degree $2p$. Hence, the modular Hadamard matrix associated with the sequence (polynomial) of the Theorem is indeed of type 1 as asserted. The correlations in degrees $\equiv 0 \mod 4$ are $2(p-1)$. Note that the correlation in degree $p$ is $2(p-1)\,\varepsilon_0\,\varepsilon_1$ because $z^p+z^{-p}$ also appears in the sum $\sum_{\nu=1}^{p}(z^{2\nu-1}+z^{-(2\nu-1)})$ for $\nu = \frac{p+1}{2}$.

REMARK. It seems probable, from computer-assisted experimentation, that $p-1$ may be the maximum modulus for a modular circulant Hadamard matrix of type 1 and size $4p$. However, the power of 2 dividing $p-1$ is certainly not always maximal as the power of 2 dividing the modulus of a modular CHM of type 1 and size $4p$. There are many values of $p$ (where $p$ is prime and satisfies $p \equiv 9 \mod 16$) for which a variant of the formula for $H(z)$ in the above Theorem yields a 16-modular CHM. The first few such values of $p$ are $p = 73,\ 89,\ 233,\ \ldots$. On the other hand, it seems for example that indeed no 16-modular, type 1 CHM of size $4p$ exists for $p = 41$.

We hope to come back on the general question of 16-modular circulant Hadamard matrices of type 1 in a future publication.

## 3. CIRCULANT MODULAR HADAMARD MATRICES OF TYPE 2

In this section we produce circulant modular Hadamard matrices of type 2 and size $n = 2(q+1)$, where $q$ is an arbitrary odd prime power. The existence of such objects is a corollary of a theorem from the 1971 paper [DGS].

We are grateful to Roland Bacher for valuable discussions about some unpublished work of his which helped in obtaining the following result.

THEOREM 2. *For every $n = 2(q+1)$, where $q$ is an odd prime power, there exists a binary sequence $X = (x_0, \ldots, x_{n-1})$ with $x_i = \pm 1$ for all $i$ $(0 \le i \le n-1)$, such that $\gamma_k(X) = 0$ for all $k \neq 0, \frac{n}{2}$. In other words,* $\mathrm{circ}(X)$ *is a circulant modular Hadamard matrix of type 2 and size $n$.*