Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 187-192*

Special weight partitions modulo a prime

V. Vavrek
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
P.O. Box 323, 5000V, Tarnovo, BULGARIA
A.J. van Zanten
Delft University of Technology, Dept. of Mathematics,
P.O. Box 5031, 2600 GA Delft, THE NETHERLANDS

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. In this paper the problem of the sign of the binary Gauss sum is solved by considering partitions mod p in unequal parts of size at most $(p-1)/2$. Generalizations of this technique are developed.

1 Introduction

Let p be an odd prime. The expression $G(1) := \sum_{n=1}^{p-1} e^{2\pi in/p} = -1$ can be considered as the sum of a finite geometric series. Less elementary is the summation of $G(2) := \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{2\pi in/p} = \sum_{i=1}^{p-1} \chi(n) e^{2\pi in/p}$, where $\left(\frac{n}{p}\right)$ is the Legendre symbol, being equal to 1 if n is a quadratic residue mod p and equal to -1 otherwise. This problem is known as the determination of the quadratic Gauss sum. Gauss rather easily derived that $G(2)^2 = \left(\frac{-1}{p}\right) p$, but it was only after four more years that he determined the sign of $G(2)$. Since then many proofs have been found, linking the problem to other mathematical problems of various nature (cf. [1]). In this contribution we shall present a proof in terms of binary words representing special partitions mod p. More generally, one defines Gauss sums with respect to a field $GF(q)$, q an odd prime power, a s $G(\chi, \psi) := \sum_{c \in F} \chi(c)\psi(c)$, where χ is a multiplicative character and ψ an additive character.

2 Determination of the Gauss sum $G(2)$

From now on we write the quadratic Gauss sum as $G(2) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \xi^n$, with $\xi = e^{2\pi i/p}$. We introduce functions $S_p(x) := \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) x^n$ and $P_p(x) := \prod_{n=1}^{(p-1)/2} (x^{2n} - x^{-2n})$, $x \in \mathbb{C}$. In [3] it is proved, by applying the orthogonality relations for the additive and multiplicative group of $GF(p)$, that for all $b \in \{1, 2, \ldots, p-1\}$

$$S_p(\xi^b)^2 = P_p(\xi^b)^2 = \left(\frac{-1}{p}\right) p. \tag{1}$$

Let $\xi = \zeta^2$, where ζ denotes the primitive $(2p)^{\text{th}}$ root of unity $e^{2\pi i/(2p)}$. It follows from (1) that the algebraic numbers ζ^a, $a \in \{0, 1, \ldots, 2p-1\}$, all satisfy the equation $S_p(x)^2 - P_p(x)^2 = 0 \bmod x^p + 1$. From these properties one can derive (cf. [3]) that we have the following polynomial identity in $\mathbb{Q}[x]$

$$\prod_{n=1}^{\frac{p-1}{2}} (x^{2n} - 1) = \mu_p x^{2k} \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) x^n \bmod x^p + 1, \tag{2}$$

where $2k := (p^2-1)/8$ and with a uniquely determined constant $\mu_p \in \{-1, +1\}$. From (2) we know $G(2) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \xi^n = \mu_p \xi^{-2k} \prod_{n=1}^{\frac{p-1}{2}} (\xi^{2n}-1) = \mu_p \prod_{n=1}^{\frac{p-1}{2}} (\xi^n - \xi^{-n})$. From (1) we know $GF(p)^2 \in \{-p, +p\}$, and so $G(2) = e^{i\varphi}\sqrt{p}$. To determine φ, we remark that Re $(\xi^n - \xi^{-n}) = 0$ and Im $(\xi^n - \xi^{-n}) > 0$, for all relevant values of n. If $p = 1 \bmod 8$, the product in the rhs contains $4k$ factors of the form ai with $a > 0$ for some positive integer k. Hence, $\varphi = 0$ and $G(2) = \mu_p\sqrt{p}$ in this case. Similarly, we find $G(2) = -\mu_p\sqrt{p}$ for $p = -3 \bmod 8$, $G(2) = i\mu_p\sqrt{p}$ for $p = +3 \bmod 8$, and $G(2) = -i\mu_p\sqrt{p}$ for $p = -1 \bmod 8$.

So, the problem of the sign of $G(2)$ turns out to be equivalent to determining μ_p in the polynomial identity (2). To accomplish this, we compare the coefficients c_{2i} of some power x^{2i} in both sides of (2). Since the polynomials have to be taken modulo $x^p + 1$, we can interpret them as polynomials in x of degree at most $p-1$. Since $(p^2-1)/8$ is even if $p = \pm 1 \bmod 8$, and odd if $p = \pm 3 \bmod 8$, we can write respectively $2k = 2\kappa + 2lp$ and $2k = 2\kappa + (2l+1)p$, with $0 \le \kappa < p$. Hence, $x^{2k} = x^{2\kappa}\left(\frac{2}{p}\right)$, and the coefficient of x^{2s} in the rhs of (2) is equal to $\mu_p \left(\frac{2}{p}\right)\left(\frac{s-\kappa}{p}\right)$. By writing $\prod_{n=1}^{(p-1)/2}(x^{2n} - 1) = (-1)^{(p-1)/2} \prod_{n=1}^{(p-1)/2}(1 - x^{2n})$ for the lhs of (2), we see that for c_{2s} at the left, we have to take into account all N^s partitions of s mod p into unequal parts of size at most $(p-1)/2$. More precisely, this coefficient equals $(-1)^{(p-1)/2(N^s_{\mathbf{e}} - N^s_{\mathbf{o}})}$, where $N^s_{\mathbf{e}}$ and $N^s_{\mathbf{o}}$ denote the number of such partitions into an even number of parts and into an odd number of parts, respectively. We conclude that the remaining problem now is to determine, for at least one value of $s \neq \kappa$, whether $N^s_{\mathbf{e}} - N^s_{\mathbf{o}}$ equals $+1$ or -1. Above we proved already implicitly that the absolute value equals 1.

3 Partitions mod p in unequal parts

We introduce binary words of length $(p-1)/2$ denoted by $\boldsymbol{a} = (a_1, a_2, \ldots, a_{(p-1)/2})$. The number of ones in such a word $\mathbf{a}$ is called the *weight* of $\boldsymbol{a}$, and is denoted by $|\boldsymbol{a}|$. Furthermore, we define the *value* of $\boldsymbol{a}$ as $\text{val}(\boldsymbol{a}) := \sum_{j=1}^{(p-1)/2} j a_j \bmod p$. If s is the value of a vector $\boldsymbol{a}$ with weight k, we can say that $\boldsymbol{a}$ corresponds to a partition mod p of s into k unequal parts of size at

most $(p-1)/2$. A part of size j occurs in this partition if and only if $a_j = 1$. We also define sets containing all words with value s, $0 \le s \le p-1$, as follows

$$A_s = \left\{ \boldsymbol{a} \in \{0,1\}^{(p-1)/2} \mid \mathrm{val}(\boldsymbol{a}) = s \right\}. \tag{3}$$

It follows from Section 2 that the function $\prod_{n=1}^{(p-1)/2}(1-x^n) \bmod x^p-1$ generates the numbers $N_{\mathbf{e}}^s - N_{\mathbf{o}}^s$. Similarly, the function $\prod_{n=1}^{(p-1)/2}(1+x^n) \bmod x^p-1$ is the generator of the numbers $N^s := N_{\mathbf{e}}^s + N_{\mathbf{o}}^s$, $0 \le s < p$. If we define $\alpha := \prod_{n=1}^{(p-1)/2}(1+\xi^n)$, then $\prod_{n=1}^{p-1}(1+\xi^n) = \alpha\alpha^c$. On the other hand, we have $\prod_{n=1}^{p-1}(1+\xi^n) = \prod_{n=1}^{p-1}(x-\xi^n)\Big|_{x=-1} = \frac{x^n-1}{x-1}\Big|_{x=-1} = 1$, and so $|\alpha| = 1$.

For practical reasons, we shall from now on consider words over $\{-1,+1\}$ instead of over $\{0,1\}$. Let $\boldsymbol{b} = (b_1, b_2, \ldots, b_{(p-1)/2})$ be a word over $\{-1,+1\}$ of length $(p-1)/2$. Then we define, similarly as in Section 2, $\mathrm{val}(b) := \sum_{j=1}^{(p-1)/2} jb_j \bmod p$, and we introduce sets of all words with value $2s$, $0 \le s \le p-1$,

$$B_s = \left\{ \boldsymbol{b} \in \{-1,+1\}^{(p-1)/2} \mid \mathrm{val}(\boldsymbol{b}) = 2s \right\}. \tag{4}$$

There is a one-one correspondence between the words $\boldsymbol{a} \in A_s$ and the words $\boldsymbol{b} \in B_{s-\kappa}$ obtained by replacing each 0 in $\boldsymbol{a}$ by -1. This follows from $\mathrm{val}(\mathbf{1}) = \sum_{j=1}^{(p-1)/2} j = (p^2-1)/8 = 2\kappa$, and so $\mathrm{val}(\boldsymbol{b}) = \mathrm{val}(\boldsymbol{a}) - (\mathrm{val}(\mathbf{1}) - \mathrm{val}(\boldsymbol{a})) = 2(s-\kappa)$. We define for each $\lambda \in GF(p)\backslash\{0\}$ a map T_λ from $\{-1,+1\}^{(p-1)/2}$ onto itself by

$$T_\lambda((b_1, b_2, \ldots, b_{(p-1)/2})) = (d_1, d_2, \ldots, d_{(p-1)/2}), \tag{5}$$

$$d_i = b_{i/\lambda}, \text{ if } i/\lambda < p/2, \text{ and } d_i = -b_{p-i/\lambda}, \text{ if } i/\lambda > p/2. \tag{6}$$

An equivalent rule is that in $GF(p)$ we have $id_i = \lambda.jb_j$ for all corresponding indices i and j. From this relation it follows that T_λ defines a bijection between B_s and $B_{\lambda s}$ for any s with $0 < s \le p-1$. An immediate consequence is that all sets B_s, $s \ne 0$, have the same size. So, the same holds for all sets A_s, $s \ne \kappa$, and we can write $N := N^i$, $i \in \{0,1,\ldots,p-1\}\backslash\{\kappa\}$. These observations enable us to determine the difference $N^\kappa - N^{\kappa+1}$ up to a sign, because of the following series of equalities $\alpha = \prod_{n=1}^{(p-1)/2}(1+\xi^n) = \prod_{n=1}^{p-1} N^n\xi^n = (N^\kappa - N)\xi^\kappa$ $+N(1+\xi+\xi^2+\cdots+\xi^{p-1}) = (N^\kappa - N)\xi^\kappa$. Hence, $N^\kappa - N^{\kappa+1} = N^\kappa - N = \pm 1$. Furthermore, we have $N^\kappa + (p-1)N = 2^{(p-1)/2}$. Combining these relations gives $N = (2^{(p-1)/2}-1)/p$, $N^\kappa = N+1$ for $p = \pm 1 \bmod 8$, and $N = (2^{(p-1)/2}+1)/p$, $N^\kappa = N-1$ for $p = \pm 3 \bmod 8$. In order to calculate the difference $N_{\mathbf{e}}^s - N_{\mathbf{o}}^s$ for at least one $s \ne \kappa$, say $s = \kappa+1$, it is sufficient to determine the parity of the total number of zeros in the words of $A_{\kappa+1}$, or equivalently, the parity of the number of minus ones in the words of B_1. We shall do this in the next proof.

Theorem 1. *For any odd prime p one has $N_{\mathbf{e}}^{\kappa+1} - N_{\mathbf{o}}^{\kappa+1} = 1$.*

Proof. First we remark that together with any $\boldsymbol{b} \in B_0$ also $-\boldsymbol{b}$ occurs in B_0. Hence, the number of words in B_0 starting with 1 is equal to $N^\kappa/2$ and so is the number of words starting with -1. Changing this -1 into $+1$ gives us all words in B_1 starting with $+1$, since the words in B_1 have value 2. Let $p = \pm 3 \bmod 8$. Then, since B_1 contains $N^\kappa + 1$ words, the number of words starting with -1 is equal to $N^\kappa/2 + 1$. More generally, if i is odd B_i contains $N^\kappa/2$ words starting with $+1$ and $N^\kappa/2$ words starting with -1, while for even i these numbers must be interchanged. Hence, depending on the parity of $N^\kappa/2$, either the sets B_i with odd index or the sets B_i with even index contain an odd number of words starting with -1. The same holds if $p = \pm 1 \bmod 8$. Now, we arrange the words in any of these $(p-1)/2$ sets in some order, yielding $(p-1)/2$ blocks with N rows and $(p-1)/2$ columns. A map T_λ which maps the rows of such a block B_i to the rows of B_1, has the property that the columns of B_i are mapped to plus or minus the columns of B_1, as follows from (4). We require that the first column of B_i is transformed into column j of B_1. This is possible if and only if λ and j satisfy $\lambda j = 1$ in $GF(p)$, with $j \in \{1, 2, \ldots, (p-1)/2\}$, and λ even. An equivalent condition is $2(\lambda/2)j = 1$, $\lambda/2, j \in \{1, 2, \ldots, (p-1)/2\}$. Because of the symmetry between $\lambda/2$ and j, this equation has an odd number of solutions if and only if 2 is a quadratic residue in $GF(p)$. We conclude that block B_1 contains an odd number of entries -1, if and only if $p = \pm 1 \bmod 8$, and consequently that $A_{\kappa+1}$ contains an odd number of words with an odd number of zeros only for such p.

(i) Let $p = 1 \bmod 4$. Then the word length $(p-1)/2$ is even. From the above observations it follows that $A_{\kappa+1}$ contains an odd number of words with even parity if $p = 1 \bmod 8$ and an even number if $p = -3 \bmod 8$. Since in this case $N^{\kappa+1} (= N) = 1 \bmod 4$, it follows that $N_{\mathbf{e}}^{\kappa+1} - N_{\mathbf{o}}^{\kappa+1} = 1$.

(ii) Let $p = 3 \bmod 4$. Now we have $(p-1)/2$ is odd and $N^{\kappa+1} = 3 \bmod 4$. By similar arguments as above we find again $N_{\mathbf{e}}^{\kappa+1} - N_{\mathbf{o}}^{\kappa+1} = 1$. □

Corollary 1. (Gauss 1805) *For an odd prime p one has $G(2) = +\sqrt{p}$ if $p = 1 \bmod 4$, and $G(2) = +i\sqrt{p}$ if $p = 3 \bmod 4$.*

This follows by substituting the result of Theorem 1 into

$$\mu_p = \left(\frac{2}{p}\right)(-1)^{(p-1)/2}(N_{\mathbf{e}}^{\kappa+1} - N_{\mathbf{o}}^{\kappa+1}).$$

4 Generalization for q-ary words

Let $\sigma \in GF(p)^*$ be of order q with respect to p, i.e. $\mathrm{ord}_p(\sigma) = q$, with q a prime, then $q | p-1$. Define $R := \{1, \sigma, \ldots, \sigma^{q-1}\}$ and let $\boldsymbol{w} = (w_1, w_2, \ldots, w_{(p-1)/q})$

be a word of length $(p-1)/q$, where each w_i is some representative of an element of $GF(p)^*/R$. For any $\boldsymbol{b} \in R^{(p-1)/q}$ we define its value in $GF(p)$ as $\mathrm{val}(\boldsymbol{b}) := \sum_{j=1}^{(p-1)/q} w_j b_j$. Furthermore, we introduce sets $B_{s,q} := \{\boldsymbol{b} \in R^{(p-1)/q} \mid \mathrm{val}(\boldsymbol{b}) = s\}$. One can immediately verify that for $q = 2$, when $\sigma = p-1 (= -1)$ and $R = \{-1, +1\}$, the set $B_{2s,2}$ is identical to the set in (4) when we choose $w_j = j$ for $1 \le j \le (p-1)/2$. Similarly as in Section 2, we define for any $\lambda \in GF(p)^*$, a map from $R^{(p-1)/q}$ onto itself

$$T_\lambda((b_1, b_2, \ldots, b_{(p-1)/2})) = (d_1, d_2, \ldots, d_{(p-1)/q}), \tag{7}$$

by $w_i b_i = \lambda w_j d_j$. In the same way as in Section 3 we can prove that all sets $B_{s,q}$, $s \neq 0$, have the same size. Therefore, if $N^{s,q} := |B_{s,q}|$, $s \neq 0$, we can define $N^q := N^{s,q}$, $s \neq 0$. Just like for $q = 2$ there is a one-to-one map from words $\boldsymbol{b} = (a, b_2, \ldots, b_{(p-1)/q}) \in B_{s,q}$ to words $\boldsymbol{b'} = (1, b_2, \ldots, b_{(p-1)/q}) \in B_{s+(1-a)w_1,q}$, where $a = \sigma^i$, $0 \le i \le q-1$. From now on we take $w_1 = 1$. Let $N^{s,a,q}$ denote the number of words in $B_{s,q}$ starting with some $a \in R$, then it is clear that we have for all $s \in \{0, 1, \ldots, p-1\}$

$$\sum_{a \in GF(p)} N^{s+1-a,1,q} = N^{s,q} \tag{8}$$

We interpret (8) as a set of p linear equations for the $p-1$ unknown numbers $N^{s+1-a,1,q}$. The coefficient matrix A of this set is a circulant matrix defined by its first row, $(s = 0)$, $a_0, a_1, \ldots, a_{p-1}$, with $a_i = 1$ if $i \in \{0, \sigma - 1, \ldots, \sigma^{q-1} - 1\}$ and $a_i = 0$ otherwise.

Lemma 1. *If* $\det A$ *is even, then* $N^{0,q} - N^{1,q}$ *is even and* $N^{1,q}$ *is odd.*

Proof. Assume that $N^{0,q} - N^{1,q}$ is odd. Since $N^{0,q} + (p-1)N^{1,q} = q^{(p-1)/q}$, being the total number of words of length $(p-1)/q$ over R, and since both p and q are odd, $N^{0,q}$ is odd and $N^{1,q}$ is even. Let $\boldsymbol{b} = (b_0, b_1, \ldots, b_{p-1})$ be a binary vector such that $b_i = 1$ if and only if $N^{i,1,q}$ is odd. If we consider A as a matrix over $GF(2)$, it follows that $A\boldsymbol{b} = (1, 0, \ldots, 0)^T$. Applying the fact that A is a circulant, we can show that all rows of the identity matrix are obtained as linear combinations of the rows of A. Hence, $\det(A) \neq 0$ in $GF(2)$ However, this contradicts the assumption in the Lemma. So, $N^{0,q} - N^{1,q}$ must be even and $N^{1,q}$ must be odd. □

Lemma 2. *If* $f(x) := x^{s^2+s+1}$ *and* $g(x) := x^{s+1} + x + 1$, *with* $s := 2^k$, $k \ge 0$, *are polynomials over* $GF(2)$, *then* $g(x)$ *is a divisor of* $f(x)$.

A proof can be given by induction and by making use of a Pascal triangle modulo 2. We omit the details.

Theorem 2. *Let* $q = 3$. *If* p *is a prime of the form* $4^n + 2^n + 1$, $n > 0$, *then* $N^{0,q} - N^{1,q}$ *is even.*

Proof. First we transform A by a similarity transformation to a circulant B such that the three ones in the first row are on positions 0, 1 and $\sigma+1$. From the rule for computing the determinant of circulants, we have

$$\det B = \prod_{j=0}^{p-1}(1+\omega_j+\omega_j^{\sigma+1}) = \prod_{j=0}^{p-1}(1+\omega^j+\omega^{j(\sigma+1)}),\ \omega = e^{2\pi i/p} \qquad (9)$$

We take $\sigma = 2^n$, $n > 0$. In $GF(p)$ we then have $\sigma^2+\sigma+1 = 4^n+2^n+1 = 0 \bmod p$ and hence $\sigma^3-1 = (\sigma-1)(\sigma^2+\sigma+1) = 0$, so $q = 3$. Another consequence of this choice is $x^{\sigma^2+\sigma+1}-1 | x^p-1$. Let F be an extension field of $GF(2)$ containing all p^{th} roots ω_j of unity. From Lemma 2 it now follows that $x^{\sigma+1}+x+1$ is a divisor of x^p+1 in F and that at least one of the ω_j is a zero of $x^{\sigma+1}+x+1$. We conclude that $\det(B) = \det(A) = 0$ in F, and hence also in $GF(2)$. Lemma 1 now provides the result. □

Remarks. 1. In [4] it is shown that the integer 4^n+2^n+1 $n > 0$, can only be a prime if n is a power of 3. The three smallest primes of this type are 7, 73 and 262657.

2. Theorem 2 shows that under the required conditions 2 is a divisor of $N^{0,q}-N^{1,q}$. Similar techniques can be applied to prove the existence of prime divisors larger than 3 in some cases. The case of a prime divisor 3 must be dealt with separately. As a result we found that 3 is a divisor of $N^{0,q}-N^{1,q}$, if $p = 9^1+3^1+1$ and if $p = 9^3+3^3+1$.

3. As a byproduct of the investigations mentioned above, we were able to construct a cyclic self-orthogonal binary code of order p, if p is of the form $6k+1$ and if the corresponding number $N^{1,q}$ is even (this last condition is satisfied for almost all primes $6k+1$).

References

[1] B. Bruce, C. Berndt, R. J. Evans. The determination of Gauss sums, *Bull. Am. Math. Soc. 5 1981*, 107-129.

[2] A. J. van Zanten, V. V. Vavrek, Partitions and constant-value codes, *Proc. Eleventh Intern. Workshop ACCT*, Pamporovo, Bulgaria, June 16-22, 2008, 312-317.

[3] A. J. van Zanten, V. V. Vavrek, Gauss sums, partitions and constant-value codes, *TiCC, TilburgUniversity*, http://www.tilburguniversity.edu/research/institutes-and-research-groups/ticc/research-programs/cc/technical-reports, *to be published.*

[4] S. W. Golomb, Cyclotomic polynomials and factorization theorems, *Amer. Math. Monthly* 85, 1978, 734-737.