Codes Correcting Asymmetric/Symmetric Errors of Limited Magnitude

Jinquan Luo

Department of Informatics, University of Bergen, Norway

Joint work with Torleiv Kløve, Irina Naydenova and Somaye Yari

Outline

- Introduction
- The asymmetric case
- The symmetric case
- Conclusion

Introduction

. In the symmetric error model, a symbol a over the alphabet

$$Z_q = \{0, 1, \ldots, q-1\}$$

may be modified during transmission into another symbol $b \in Z_q$. For some applications, the error magnitude $b - a$ (asymmetric case) or $|b - a|$ (symmetric case) is not likely to exceed a certain threshold λ. One such application is the multilevel flash memory. A multilevel flash cell is electrically programmed into one of q threshold states and thus can be viewed as storing one symbol from the set $\{0, 1, \cdots, q-1\}$. Moreover, errors in this type of memory are typically in one direction and have small magnitudes that may be significantly lower than the size of the alphabet. Therefore, the limited magnitude asymmetric error model is well suited for such an application.

. A modified model, where wrap-around error are also possible, was considered in

Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, Codes for asymmetric limited-magnitude errors with application to multi-level flash memories, *IEEE Trans. Information Theory*, vol. 56, pp. 1582–1595, April 2010.

For this model, a can be changed to $(a+e) \pmod q$, where $0 \le e \le \lambda$ (asymmetric errors).

In this talk we will construct several classes of systematic codes correcting asymmetric or symmetric errors. The constructions are based on $B_t[\lambda](q)$ sets or $B_t[\pm\lambda](q)$ sets.

The main results of this talk are in

Torleiv Kløve, Jinquan Luo, Irina Naydenova and Somaye Yari, Some codes correcting asymmetric errors of limited magnitude, *IEEE Trans. Information Theory*, vol. 57, pp. 7459–7472, Nov. 2011.

Torleiv Kløve, Jinquan Luo, and Somaye Yari, Codes correcting single errors of limited magnitude, *IEEE Trans. Information Theory*, vol. 58, pp. 2206–2219, April 2012.

Code Construction Here we consider linear codes over the ring Z_q of integers module q. If H is an $r \times m$ matrix over Z_q, the corresponding code of length m is

$$C_H = \left\{ \mathbf{x} \in Z_q^m \,|\, \mathbf{x}H^t = 0 \right\}$$

where H^t denotes the transpose of H. If q is a prime, then C_H is a vector space, in general it is a module.

Let $\mathcal{E} \subset Z_q^m$ be the set of error patterns that we want to correct. If $\mathbf{x}$ is a sent codeword and $\mathbf{e}$ is an error introduced during transmission, then the received m-tuple is $\mathbf{y} = \mathbf{x} + \mathbf{e}$. Then the syndrome of $\mathbf{e}$ is

$$\mathbf{y}H^t = \mathbf{x}H^t + \mathbf{e}H^t = \mathbf{e}H^t.$$

Let

$$\mathcal{S}_{H,\mathcal{E}} = \left\{\mathbf{e}H^t \,|\, \mathbf{e} \in \mathcal{E}\right\}$$

be the set of syndromes. The code is able to correct all error patterns in $\mathcal{E}$ if and only if all the syndromes are distinct, i.e., $|\mathcal{S}_{H,\mathcal{E}}| = |\mathcal{E}|$. When this is the case, the code is able to correct all error patterns in $\mathcal{E}$. Moreover

$$\bigcup_{\mathbf{x}\in C_H} \{\mathbf{x} + \mathbf{e} \,|\, \mathbf{e} \in \mathcal{E}\}$$

is a disjoint union. So we get the Hamming bound

$$|C_H| \cdot |\mathcal{E}| \leq q^m.$$

For ordinary linear codes (for prime q), when $r = 1$, C_H is an $[m, m-1]$ code of Hamming distance 2 which can not correct any errors (without limitation on the magnitude of errors). When we consider errors of limited magnitude, the situation maybe quite different. If the error patterns are mainly the set of sequences $(e_0, \cdots, e_{m-1}) \in [0, \lambda]^m$ (asymmetric case) of Hamming weight at most t. We denote this set by $\mathcal{E}_{\lambda,m}$. Then

$$|\mathcal{E}_{\lambda,m,t}| = \theta(\lambda, m, t) := \sum_{u=0}^{t} \binom{m}{u} \lambda^u.$$

Then we consider sets

$$B = \{b_0, b_1, \cdots, b_{m-1}\}$$

of distinct positive integers and

$$H = (b_0, b_1, \cdots, b_{m-1})$$

such that the corresponding syndromes

$$\mathcal{S}=\left\{\sum_{j=0}^{m-1} e_j b_j \bmod q \,|\, (e_0,e_1,\cdots,e_{m-1})\in\mathcal{E}_{\lambda,m,t}\right\}$$

are distinct. This B is called a $B_t[\lambda](q)$ set. The corresponding code we denote by C_B, that is

$$C_B=\left\{(x_0,x_1,\cdots,x_{m-1})\in Z_q^m \mid \sum_{i=0}^{m-1} x_i b_i \equiv 0 \bmod q\right\}.$$

In particular, if $\gcd(b_0,b_1,\cdots,b_{m-1},q)=1$, then $|C_B|=q^{m-1}$. If we have equality in the Hamming bound, then $\theta(\lambda,m,t)=|\mathcal{S}|=q$. In this case we call C_B a perfect code and B a perfect $B_t[\lambda](q)$ set.

Another construction of H for correction single error with arbitrary values of r is: if B is a $B_1[\lambda](q)$ set, $\gcd(q,\lambda!)=1$, and H is an

$r \times m(q^r - 1)/(q-1)$ matrix whose columns are all possible vectors in Z_q^r whose first entry belongs to B, then C_H can correct a single error of magnitude at most λ.

The symmetric case is similar. Therefore the construction of codes correcting errors of limited magnitude leads to the study of $B_t[\lambda](q)$ set (asymmetric case) or $B_t[\pm\lambda](q)$ set (symmetric case).

The Asymmetric case

$\boxed{B_m[\lambda](q) \text{ sets of size } m}$ For integers a, b, where $a \leq b$, we use the notation

$$[a, b] = \{a, a+1, \cdots, b\}.$$

The case $t = m$ is very simple. We have $\theta(\lambda, m, m) = (\lambda+1)^m$ and for any $q \geq (\lambda+1)^m$,

$$\{(\lambda+1)^i \,|\, 0 \leq i \leq m-1\}$$

is a $B_m[\lambda](q)$ set since for any $a \in [0, (\lambda+1)^m - 1]$ has a unique expansion

$$a = \sum_{i=0}^{m-1} x_i (\lambda+1)^i$$

where $x_i \in [0, \cdots, \lambda]$.

$\boxed{B_{m-1}[\lambda](q) \text{ sets of size } m}$ We have

$$\theta(\lambda, m, m-1) = (\lambda+1)^m - \lambda^m.$$

We give a collection of $B_{m-1}[\lambda](q)$ sets for some specific q. Let $p = 2\nu + 1$ and $\Lambda = \lambda + \nu + 1$.

Theorem 1. *If $\Lambda > p$ and $\gcd(\Lambda, p) = 1$, then*

$$\left\{\Lambda^i(\Lambda - p)^{m-1-i} \,|\, i \in [0, m-1]\right\}$$

is a $B_{m-1}[\lambda](q)$ set, where

$$q = \sum_{i=0}^{m-1} \Lambda^i(\Lambda - p)^{m-1-i} = \frac{\Lambda^m - (\Lambda - p)^m}{p}.$$

We note that for $\nu = 0$ we get $q = (\lambda+1)^m - \lambda^m$, that is, the set

$$\left\{(\lambda+1)^i \lambda^{m-1-i} \,|\, i \in [0, m-1]\right\}$$

is perfect.

On $B_1[2](q)$ set

In the following we will study the case $t = 1$ which means that the corresponding code can correct single asymmetric error of magnitude at most λ. Define $M_\lambda(q)$ to be the maximal size of a $B_1[\lambda](q)$ set.

Firstly, since

$$q \geq \theta(\lambda, m, 1) = 1 + m\lambda$$

we have

$$m \leq \lfloor \frac{q-1}{\lambda} \rfloor.$$

A $B_1[\lambda](q)$ set of size $\lfloor (q-1)/\lambda \rfloor$ is called quasi-perfect. In particular, if $\lambda \mid (q-1)$, then the set is perfect.

Now we will calculate $M_2(q)$ and also give the construction of maximal size $B_1[2](q)$ set.

For a prime p and an integer n, the p-adic exponent valuation of n, denoted by $v_p(n)$, is the exact power of p dividing n, that is, $n = p^{v_p(n)}n'$ where $p \nmid n'$.

For any positive integer l coprime to d, let $\mathrm{ord}_d(l)$ be the order of l in $Z_d^* = \{a \mid \gcd(a, d) = 1, 1 \leq a \leq d-1\}$.

Let P_o be the set of odd primes p such that $\mathrm{ord}_p(2)$ id odd. For odd q, if

$$q = p_1^{t_1} \cdots p_s^{t_s}$$

is the prime factorization of q, let

$$q_o = \prod_{\substack{1 \leq i \leq s \\ p_i \in P_o}} p_i^{t_i}. \tag{1}$$

Theorem 2. *(1). If q is odd, then*

$$M_2(q) = \frac{q-1}{2} - \sum_{d|q_o, d>1} \frac{\varphi(d)}{\mathrm{ord}_d(2)}$$

where $\varphi(d) = |Z_d^*|$ is the Euler function. In particular, perfect $B_1[2](q)$ sets exist if and only if none of the primes dividing q belongs to P_o.

*(2). (**T.Kløve, B. Bose, and N. Elarief**) For all $m \geq 0$, we have $M_2(4m+2) = 2m$, that is, there are quasi-perfect $B_1[2](4m+2)$ sets.*

*(3). (**T.Kløve, B. Bose, and N. Elarief**) For all $m \geq 1$, we have*

$$M_2(4m) = m + M_2(m).$$

Example 1. *Let* $q = 50715 = 3^2 \cdot 5 \cdot 7^2 \cdot 23$. *We have*

$$\begin{aligned} \mathrm{ord}_3(2) &= 2, \quad \mathrm{ord}_5(2) = 4, \\ \mathrm{ord}_7(2) &= 3, \quad \mathrm{ord}_{23}(2) = 11. \end{aligned}$$

Hence $3, 5 \notin P_o$ *and* $7, 23 \in P_o$. *Therefore,* $q_o = 7^2 \cdot 23$. *Then we have*

$$\begin{aligned} &\mathrm{ord}_{7^2}(2) = 3 \times 7 = 21, \\ &\mathrm{ord}_{7\cdot 23}(2) = l.c.m(3, 11) = 33, \\ &\mathrm{ord}_{7^2\cdot 23}(2) = l.c.m(21, 11) = 231. \end{aligned}$$

Hence

$$\begin{aligned} M_2(50715) &= \tfrac{50715-1}{2} - \left(\tfrac{\varphi(7)}{\mathrm{ord}_7(2)} + \tfrac{\varphi(23)}{\mathrm{ord}_{23}(2)} + \tfrac{\varphi(7^2)}{\mathrm{ord}_{7^2}(2)} + \tfrac{\varphi(7\cdot 23)}{\mathrm{ord}_{7\cdot 23}(2)} + \tfrac{\varphi(7^2\cdot 23)}{\mathrm{ord}_{7^2\cdot 23}(2)} \right) \\ &= \tfrac{50715-1}{2} - \tfrac{14}{2} = 25350. \end{aligned}$$

$\boxed{\text{On } B_1[\lambda](p) \text{ for primes } p}$ Let $p > \lambda$ be a prime and g be a primitive element in the field Z_p. Define

$$H_\lambda =< 2, 3, \cdots, \lambda >_p$$

to be the multiplicative group in Z_p^* generated by $2, 3, \cdots, \lambda$. Assume the cardinality of H is n. Since Z_p^* is cyclic, then $H_\lambda =< h >_p$ where $h = g^{(p-1)/n}$. Define

$$\mathrm{ind}_h(j) = \min\{a \,|\, a > 0, h^a \equiv j \pmod{p}\}.$$

On $B_1[\lambda](p)$ for primes p

Theorem 3. *Let $\lambda \geq 2$. If p is a prime, $\lambda \mid n$ and*

$$\{\mathrm{ind}_h(j) \bmod \lambda \mid 2 \leq j \leq \lambda\} = [1, \lambda - 1],$$

then

$$B = \{g^{(p-1)\lambda i/n+j} \mid 0 \leq i \leq n/\lambda - 1,\ 0 \leq j \leq (p-1)/n - 1\}$$

is a perfect $B_1[\lambda](p)$ set.

Furthermore, in the case $\lambda = 3$, the converse of this theorem also holds.

Theorem 4. *If p is a prime, then a prefect $B_1[3](p)$ set exists if and only if 3 divides n and*

$$\{\mathrm{ind}_h(2) \bmod 3\ , \mathrm{ind}_h(3) \bmod 3\} = [1, 2].$$

On $B_1[3](2^kr)$ sets Suppose $q = 2^kr$ with $(6, r) = 1$. Now we will introduce a result reducing the construction of maximal size $B_1[3](2^kr)$ set to the construction of maximal size $B_1[3](2^{k-2}r)$ set.

Define v_2 to be 2-adic exponent valuation, i.e., $v_2(n) = i$ if and only if $n = 2^in'$ with n' odd. Suppose r has the following factorization

$$r = r_0r_1 \cdots r_s \tag{2}$$

where $r_i = \prod_{j=1}^{m_i} p_{i,j}^{e_{i,j}}$ with $p_{i,j}$ distinct prime and $v_2(\mathrm{ord}_{p_{i,j}}(3)) = i$ for $0 \le i \le s$ and $1 \le j \le m_i$.

On $B_1[3](2^k r)$ sets

Theorem 5. *If r is comprime to 6 and $k \geq 2$, then*

(1). in the case $k = 2, 3$, we have $M_3(2^k r) = 2^{k-2} r + M_3(2^{k-2} r)$.

(2). in the case $k \geq 4$, we have

$$M_3(2^k r) = 2^{k-2} r - 2 \sum_{d | r_0 r_1 \cdots r_{k-3}} \varphi(d)/(\mathrm{ord}_d(3))_o + M_3(2^{k-2} r)$$

where $(\mathrm{ord}_d(3))_o$ is the odd part of $\mathrm{ord}_d(3)$ as defined in (1).

***Corollary* 1.** *Assume $q = 2^k r$ with $(6, r) = 1$. Then perfect (quasi-perfect, resp.) $B_1[3](q)$ set exists if and only if $k = 2$ or 3 and perfect (quasi-perfect, resp.) $B_1[3](2^{k-2} r)$ set exists.*

Example 2. *For $q = 20$, we have $k = 2$ and $r = 5$. Then r has two divisors: $d = 1$ or 5. Choose $T_1 = \{5\}$ and* $T_5 = \{3^{2i}|0 \leq i \leq 1\} \bigcup \{3^{2i+1} \cdot 11|0 \leq i \leq 1\} \pmod{20} = \{1, 9, 17, 13\}$. *We can choose $\{1\}$ as a quasi-perfect $B_1[3](5)$ set. Then*

$$T_1 \cup T_5 \cup 4 \cdot \{1\} = \{1, 4, 5, 9, 13, 17\}$$

is a maximal size $B_1[3](20)$ set which is also quasi perfect.

On $B_1[3](3^l r)$ sets Assume $q = 3^l r$ with $l \geq 2$, in the following we will reduce the constructions of $B_1[3](3^l r)$ set to the construction of $B_1[3](3^{l-2} r)$ set.

Theorem 6. *If r is comprime to 6 and $k \geq 2$, then we have $M_3(3^l r) = 2 \cdot 3^{l-2} r + M_3(3^{l-2} r)$.*

***Corollary* 2.** *For $q = 3^l r$ with l odd and $(r, 6) = 1$, then*

$$M_3(q) = \frac{q+r}{4} - 1.$$

Example 3. *For $q = 45$, we have $M_3(45) = 10 + M_3(5) = 11$. Indeed, we could choose*

$$\{1, 4, 5, 7, 9, 28, 32, 38, 40, 41, 44\}$$

as a maximal size $B_1[3](45)$ *set of cardinality* 11*.*

$\boxed{\text{On } B_1[4](2r) \text{ set for } \gcd(r,6)=1}$

Let d be a divisor of r and

$$t_{1,d} = \min\{n | n > 0, 2^n \in < 3 >_d\},$$

$$t_{2,d} = \min\{m | m \geq 0, 2^{t_{1,d}} \equiv 3^m \bmod d\}.$$

Theorem 7. *Suppose r is coprime to 6. If for every divisor $d > 1$ of r, $t_{2,d}$ is odd and $\mathrm{ord}_d(3)$ is even, then quasi-perfect $B_1[4](2r)$ set exists, that is, $M_4(2r) = \frac{r-1}{2}$.*

Example 4. *In the case $q = 38$: $\mathrm{ord}_{19}(3) = 18$ is even. Since $2 \equiv 3^7 \pmod{19}$, we have $t_{1,19} = 1$, $t_{2,19} = 7$ (odd) and $M_4(38) = \frac{19-1}{2} = 9$. Indeed, we could choose $\{1, 5, 7, 11, 17, 23, 25, 35\}$ as a maximal $B_1[4](38)$ set.*

$\boxed{\text{On } B_1[4](3^l r) \text{ set}}$ Assume $q = 3^l r$ with $l \geq 2$ and r coprime to 6.

Theorem 8. *If r is comprime to 6 and $l \geq 2$, then we have*

$$M_4(3^l r) = \begin{cases} 2 \cdot 3^{l-2} r - \sum\limits_{d|r, d>1} \frac{2 \cdot 3^{l-2} \varphi(d)}{l.c.m(2 \cdot 3^{l-2}, \mathrm{ord}_d(2))} + M_4(3^{l-2} r) & \text{if } l > 2, \\ 2 \cdot 3^{l-2} r - \sum\limits_{d|r, d>1, 3|\mathrm{ord}_d(2)} \frac{2\varphi(d)}{l.c.m(2, \mathrm{ord}_d(2))} + M_4(3^{l-2} r) & \text{if } l = 2. \end{cases} \tag{3}$$

***Corollary* 3.** *For $q = 9r$ with $(r, 6) = 1$, suppose for any prime divisor p of r, $3 \nmid \mathrm{ord}_p(2)$. Then*

$$M_4(9r) = 2r + M_4(r).$$

In particular, in this case, perfect (or quasi-perfect, resp.) $B_1[4](9r)$ set *exists if only only if perfect perfect (or quasi-perfect, resp.)* $B_1[4](r)$ *set exists.*

Example 5. $q = 45$*: since* $\mathrm{ord}_5(2) = 4$ *is not a multiple of* 3*, then* $M_4(45) = 10 + M_4(5) = 11$*. Indeed, we could choose*

$$\{1, 5, 7, 8, 9, 11, 17, 19, 29, 40, 43\}$$

which is an optimal $B_1[4](45)$ *set.*

Symmetric Case

In the symmetric case the error patterns are the set of sequences $(e_0, \cdots, e_{m-1}) \in [-\lambda, \lambda]^m$ of Hamming weight at most t. We denote this set by $\mathcal{E}_{\pm\lambda,m,t}$. Then

$$|\mathcal{E}_{\pm\lambda,m,t}| = \theta(\lambda, m, t) := \sum_{u=0}^{t} \binom{m}{u} (2\lambda)^u .$$

Then we consider sets

$$B = \{b_0, b_1, \cdots, b_{m-1}\}$$

of distinct positive integers such that the corresponding syndromes

$$0 \notin \mathcal{S} = \{ \sum_{j=0}^{m-1} e_j b_j \bmod q \,|\, (e_0, e_1, \cdots, e_{m-1}) \in \mathcal{E}_{\pm\lambda,m,t} \}$$

are distinct. The set B is called a $B_t[\pm\lambda](q)$ set. The corresponding code we denote by C_B, that is

$$C_B = \{(x_0, x_1, \cdots, x_{m-1}) \in Z_q^m \,|\, \sum_{i=0}^{m-1} x_i b_i \equiv 0 \bmod q\}.$$

In the following we only consider $t = 1$. In this case, since $q \geq 1 + 2m\lambda$, we have

$$m \leq \lfloor \frac{q-1}{2\lambda} \rfloor.$$

A $B_1[\pm\lambda](q)$ set of size $\lfloor(q-1)/(2\lambda)\rfloor$ is called quasi-perfect. In particular, if $2\lambda \mid (q-1)$, then the set is perfect. In this case the corresponding code is also quasi-perfect or perfect with respect to Hamming bound.

$\boxed{B_t[\lambda](q) \text{ sets from } B_t[\pm\lambda](q) \text{ sets}}$

For a $B_t[\pm\lambda](q)$ set B, define

$$\pm B = B \cup \{(-b) \bmod q \mid b \in B\}.$$

Theorem 9. • *If B is a $B_t[\pm\lambda](q)$ set, then $\pm B$ is a $B_t[\lambda](q)$ set.*

- *If B is a perfect $B_t[\pm\lambda](q)$ set, then $\pm B$ is a perfect $B_t[\lambda](q)$ set.*

- *If B is a quasi-perfect $B_t[\pm\lambda](q)$ set, then $\pm B$ is a quasi-perfect $B_t[\lambda](q)$ set.*

On perfect $B[\pm\lambda](p)$ sets for primes p

For an odd prime p, a primitive root g modulo p. Let

$$\mu = \mu_{\lambda,p} = \gcd\left(\mathrm{ind}_g(-1), \mathrm{ind}_g(2), \mathrm{ind}_g(3), \ldots, \mathrm{ind}_g(\lambda)\right).$$

That the set

$$H = \{g^{i\mu} \bmod p \mid i \geq 0\}$$

is the multiplicative subgroup of Z_p^* generated by the integers $-1, 2, 3, \ldots, \lambda$. The size of H is $n = (p-1)/\mu$. In particular, μ does not depend on g.

On perfect $B[\pm\lambda](p)$ sets for primes p

Theorem 10. *Let $\lambda \geq 2$. Let p be a prime such that $p \equiv 1 \pmod{2\mu\lambda}$, where $\mu = \mu_{\lambda,p}$. Let g be a primitive root modulo p. If*

$$\left\{\frac{\mathrm{ind}_g(j)}{\mu} \bmod 2\lambda \mid j \in [-\lambda, -1] \cup [1, \lambda]\right\} = [0, 2\lambda - 1],$$

and ν is a positive integer such that $\nu | \mu$ and $\gcd(\mu/\nu, 2\lambda) = 1$, then

$$X = \left\{g^{2\nu\lambda i + j} \bmod p \mid i \in \left[0, \frac{p-1}{2\nu\lambda} - 1\right], j \in [0, \nu - 1]\right\}$$

is a perfect $B_1[\pm\lambda](p)$ set.

On perfect $B[\pm\lambda](p)$ sets for primes p

Example 6. *Let $\lambda = 3$ and $p = 37$. Then $g = 2$ is a primitive root and $\mu = 1$. Hence*

$$B = \{2^{3i} \bmod 37 \mid 0 \leq i \leq 5\} = \{1, 8, 27, 31, 26, 23\}$$

is a perfect $B_1[\pm 3](37)$ set.

On quasi-perfect $B_1[\pm\lambda](\lambda p)$ sets for some primes p

Theorem 11. *Let* $p \equiv 3 \pmod 4$ *be a prime and* $a \equiv 1 \ (\mathrm{mod}\ \lambda)$ *such that* $\mathrm{ord}_p(a) = \frac{p-1}{2}$. *If* $i(\lambda - i)$ *is quadratic residue mod* p *for* $1 \le i < \lambda/2$, *then the set*

$$\left\{a^i \,|\, 0 \le i < (p-1)/2\right\}$$

is a quasi perfect $B_1[\pm\lambda](\lambda p)$ *set.*

NB: we can find a satisfying the preceding condition by Chinese Remainder Theorem.

By quadratic reciprocity law, we have the following observation:

- If $\lambda = 2$, we have $p \equiv 3 \pmod 4$. For primes $p = 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79$, the quasi perfect $B_1[\pm 2](2p)$ sets exist.

- If $\lambda = 3$, we have $p \equiv 7 \pmod 8$. In fact, for primes $p = 7, 23, 31, 47, 71, 79, 103, 127$, the quasi perfect $B_1[\pm 3](3p)$ sets exist.

- If $\lambda = 4$, we have $p \equiv 11 \pmod{12}$. For primes $p = 11, 23, 31, 47, 59, 71, 83, 107$, the quasi perfect $B_1[\pm 4](4p)$ sets exist.

- $\lambda = 5$, we have $p \equiv 19, 23 \pmod{24}$. For primes $p = 19, 23, 43, 47, 67, 71, 139$, the quasi perfect $B_1[\pm 5](5p)$ sets exist.

Combining two B sets into a new B sets

Define $N_\lambda(q)$ to be the maximal size of a $B_1[\pm\lambda](q)$ set.

Theorem 12. *Let B_1 be a $B_1[\pm\lambda](q_1)$ set and B_2 be a $B_1[\pm\lambda](q_2)$ set where $\gcd(\lambda!, q_2) = 1$. Let*

$$B_1 \bigodot B_2 = \{c + rq_1 \,|\, c \in B_1, r \in [0, q_2 - 1]\} \cup \{q_1 c \,|\, c \in B_2\}.$$

Then

a) $B_1 \bigodot B_2$ *is a* $B_1[\pm\lambda](q_1 q_2)$ *set.*

b) $|B_1 \bigodot B_2| = q_2|B_1| + |B_2|$.

c) $N_\lambda(q_1 q_2) \geq q_2 N_\lambda(q_1) + N_\lambda(q_2)$.

***Corollary* 4.**

- *Let B_1 be a perfect $B_1[\pm\lambda](q_1)$ set, B_2 be a $B_1[\pm\lambda](q_2)$ set and $\gcd(\lambda!, q_2) = 1$. Then $B_1 \bigodot B_2$ is perfect (or quasi-perfect, resp.) if and only if B_2 is perfect (or quasi-perfect, resp.).*

- *For any q with $\gcd(\lambda!, q) = 1$,*

$$N_\lambda((2\lambda + 1)q) \geq q + N_\lambda(q).$$

Moreover, perfect (or quasi-perfect, resp.) $B_1[\pm\lambda]((2\lambda + 1)q)$ set exists if and only if perfect (or quasi-perfect, resp.) $B_1[\pm\lambda](q)$ set exists.

- *In particular, if q is a prime, $\lambda < q < 2\lambda$, then*

$$N_\lambda((2\lambda+1)) = q$$

and

$$\{r(2\lambda+1)+1 \,|\, r \in [0, q-1]\}$$

is a quasi-perfect $B_1[\pm\lambda]((2\lambda+1)q)$ set.

On maximal $B_1[\pm 2](q)$ set

For odd q, we have the following factorization

$$q = q_0 q_1 \cdots q_s \tag{4}$$

where $q_i = \prod_{j=1}^{r_i} p_{i,j}^{e_{i,j}}$ with $p_{i,j}$ distinct prime and $v_2(\mathrm{ord}_{p_{i,j}}(2)) = i$ for $0 \le i \le s$ and $1 \le j \le r_i$.

On maximal $B_1[\pm 2](q)$ set

Theorem 13. • *For q odd, we have*

$$N_2(q) = \frac{q-1}{4} - \frac{1}{4}\left(\sum_{d|q_0} \frac{\varphi(d)}{\mathrm{ord}_d(2)} + 2\sum_{d|q_1} \frac{\varphi(d)}{\mathrm{ord}_d(2)}\right)$$

where q_0, q_1 is defined in (4).

- *The set $S = \{1, 3, \cdots, 2m-1\}$ is a quasi-perfect $B_1[\pm 2](4m+2)$ set and*

$$N_2(4m+2) = m.$$

- *For $m > 1$, we have $N_2(4m) = \lfloor \frac{m}{2} \rfloor + N_2(m)$.*

Examples

Table 1:

primes p	$\mathrm{ord}_p(2)$	$v_2(\mathrm{ord}_p(2))$
3	2	1
5	4	2
7	3	0
11	10	1
13	12	2

Example 7. *For $q = 21$, we have*

$$N_2(21) = \frac{21-1}{4} - \frac{1}{4}\left(2 \cdot \frac{\varphi(3)}{\mathrm{ord}_3(2)} + \frac{\varphi(7)}{\mathrm{ord}_7(2)}\right) = 4.$$

Indeed,

$$S = 3 \cdot \{1\} \cup \{1, 2^2, 2^4\} = \{1, 3, 4, 16\}$$

is a maximal size $B_1[\pm 2](21)$ set.

$\boxed{\text{On } B_1[\pm 3](q) \text{ sets}}$ The first q such that perfect or quasi-perfect $B_1[\pm 3](q)$ set exists are listed in the following table.

Table 2:

q	$N_3(q)$	$B_1[\pm 3](q)$ set B_q	type	
$7-12$	1	1	Q	Done
17	2	$\{1,4\}$	Q	Done
18	2	$\{1,4\}$	Q	
21	3	$\{1,4,5\}$	Q	Done
35	5	$\{1,5,6,8,13\}$	Q	Done
37	6	$\{1,6,8,10,11,14\}$	P	Done

Quasi-perfect $B_1[\pm 4](2q)$ sets for some primes q

Theorem 14. *Let $q \equiv 1 \pmod 4$ be a prime g be an odd primitive element of Z_q. If both $\mathrm{ind}_g(2)$ and $\mathrm{ind}_g(3)$ are odd,*

then the set

$$\{g^{2i} \,|\, 0 \le i < (q-1)/4\}$$

is a quasi perfect $C[4](2q)$ set.

Example 8. *Let $p = 29$. Choose $g = 11$. Then $\mathrm{ind}_g(2) = 9$ and $\mathrm{ind}_g(3) = 17$. Therefore, since $g^2 = 5 \pmod{58}$, we get the following $B_1[\pm 4](58)$ set:*

$$\{1, 5, 5^2, 5^3, 5^4, 5^5, 5^6\} \pmod{58} = \{1, 5, 25, 9, 45, 51, 23\}.$$

On $B_1[\pm\lambda](q)$ sets of size 2 and 3

Theorem 15. *The minimal q for which a $B_1[\pm\lambda](q)$ set of size 2 exists is*

$$q = (\lambda+1)^2 + 1.$$

In this case

$$B = \{1, \lambda+1\}$$

is such a set.

***Conjecture* 1.** *The minimal q for which a $B_1[\pm\lambda](q)$ set of size 3 exists is*

$$q = (\lambda+1)(\lambda+2)+1 = \lambda^2 + 3\lambda + 3.$$

In this case

$$B = \{1, \lambda+1, \lambda+2\}$$

is such a set.

Conclusion

. In this talk we discussed the construction of codes to correct asymmetric/symmetric errors of limited magnitude. The code construction is based on $B_t[\lambda](q)$ set (asymmetric) or $B_t[\pm\lambda](q)$ set (symmetric). The code is perfect or quasi perfect w.r.t Hamming bound provided that the corresponding set is perfect or quasi-prefect.

After computer search using back-tracing algorithm, we characterize several maximal size $B_t[\lambda](q)$ and $B_t[\pm\lambda](q)$ sets , in particular perfect or quasi-perfect sets. Most results concern the case $t = 1$ except for only one asymmetric case.

Not much is known for the case $t \geq 2$ which means the corresponding code can correct more that one error of limited magnitude.

Thanks!