AICR · OPEN PROBLEM

Quasi-Abelian Codes Meet the Gilbert-Varshamov Bound as the Group Grows

Known for cyclic groups, and for arbitrary abelian groups in the other asymptotic regime; the case the security of QA-SD actually needs is neither

Status. Statement: AI-written from Maxime Bombar, Geoffroy Couteau, Alain Couvreur and Clément Ducros, *Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding*, IACR ePrint 2023/845, CRYPTO 2023. Not yet checked by a human. The source names the direction and says the development is out of reach of the article, leaving it as a conjecture; it does not print a formal statement, so the formalisation below is this statement's reading and is flagged as such. Partially settled since: concrete non-asymptotic bounds are now known for particular groups, and the general asymptotic question is restated as open in that follow-up.

Category. *Coding theory; code-based assumptions.*

Conjecture (informal). *Modern silent secure computation runs on pseudorandom correlation generators, and those rest on the hardness of decoding a structured code — here, a quasi-abelian code over a group algebra. Essentially every known attack on such assumptions is a linear test, and resistance to all linear tests reduces to one purely combinatorial fact: a random code from the family has large minimum distance. Two regimes are available. Fix the group and let the number of blocks grow, and the fact is a theorem of Fan and Lin. Let the group itself grow, which is the regime the cryptographic parameters actually live in, and it is a theorem only when the group is cyclic, due to Gaborit and Zémor. The conjecture is that the cyclic restriction can be dropped.*

1 The setting

Let G be a finite abelian group and $\mathbb{F}_q[G]$ its group algebra, the $\mathbb{F}_q$-vector space with basis G and multiplication induced by the group law. An $\mathbb{F}_q[G]$-submodule of $(\mathbb{F}_q[G])^\ell$ is a *quasi-G code of index ℓ*; for G cyclic these are the quasi-cyclic codes, and for G trivial they

are all linear codes. A quasi-G code of rank k is the row space of a matrix $\Gamma \in (\mathbb{F}_q[G])^{k\times\ell}$, and Γ is *systematic* if $\Gamma = (I_k \mid \Gamma')$. As a code over $\mathbb{F}_q$ its length is $\ell \cdot |G|$ and its rate is $r = k/\ell$.

The *quasi-abelian syndrome decoding* problem QA-SD is syndrome decoding for such codes, with the parity-check matrix in systematic form. It generalises both plain and quasi-cyclic syndrome decoding, the latter being the assumption behind the NIST round-4 submissions BIKE and HQC.

Theorem 1 (Security against linear tests reduces to distance, [BCCD23, §4.5]). *If the parity-check matrix H of a quasi-G code has the property that the code generated by H has large minimum distance with high probability over the choice of H, then* QA-SD *resists every attack in the linear test framework.*

So everything turns on the minimum distance of a random quasi-G code, and there are two ways to send it to infinity.

Theorem 2 (Fixed group, growing index, [FL15, Thm. 2.1]). *Let G be a finite abelian group and $(C_\ell)_\ell$ a sequence of random quasi-G codes of index ℓ and rate $r \in (0,1)$. For $\delta \in (0, 1 - 1/q)$,*

$$\lim_{\ell\to\infty} \Pr\left[\frac{d_{\min}(C_\ell)}{|G|} > \delta\ell\right] = \begin{cases} 1 & \text{if } r < 1 - h_q(\delta), \\ 0 & \text{if } r > 1 - h_q(\delta), \end{cases}$$

both limits converging exponentially fast, over the uniform choice of a generator matrix $\Gamma_\ell \in (\mathbb{F}_q[G])^{k\times\ell}$.

Fan and Lin's result is asymptotic in ℓ with G fixed, and the source records why that is the wrong way round for its purpose: "the exponent depends on $|G|$: the larger the group G, the higher this probability". Cryptographic parameters have k and ℓ small — often $k = 1$, ℓ a small constant — and $|G|$ large.

In that regime the corresponding statement is a theorem only for cyclic G: Kasami gave a Gilbert-Varshamov-like bound for rate-1/2 quasi-cyclic codes, and Gaborit and Zémor showed various families of random double-circulant codes asymptotically satisfy a logarithmic improvement on it.

2 Notation and parameters

- G is a finite abelian group, $|G| \to \infty$ along the family; q is the field size, fixed.
- k is the rank and ℓ the index of the code, both constant; $r = k/\ell$ is the rate. The code has length $\ell \cdot |G|$ over $\mathbb{F}_q$.
- h_q is the q-ary entropy function, and $r < 1 - h_q(\delta)$ is the Gilbert-Varshamov condition.
- *Systematic* means the parity-check matrix is $(I_k \mid \cdot)$ over $\mathbb{F}_q[G]$; this is not cosmetic, see Remark 2.

3 The conjecture

Conjecture 1 ([BCCD23, §1.2, §4.5]). *Theorem 2 holds in the other asymptotic regime, for every abelian G rather than only cyclic G. Concretely: fix q, constants $k < \ell$ with $r = k/\ell$, and $\delta \in (0, 1-1/q)$ with $r < 1 - h_q(\delta)$. Then for any family of finite abelian groups G with $|G| \to \infty$, a random systematic quasi-G code of rank k and index ℓ over $\mathbb{F}_q$ satisfies $d_{\min} > \delta \cdot \ell \cdot |G|$ with probability tending to 1.*

Remark 1 (How the source states it, and what is being supplied here). The source states the direction twice and prints no formal statement. Page 9: "We conjecture an extension of Gaborit and Zémor result to arbitrary abelian groups. The latter conjecture entails that the QA-SD problem cannot be broken by any attack from the linear test framework, for any choice of the underlying group G." Page 20: "Actually, to assert the resistance of QA-SD against linear attacks, it would be more relevant to consider the regime where k, ℓ are constant and $|G|$ goes to infinity as it is done in [GZ06] but such a development is out of reach of this article and we leave it as a conjecture."

Conjecture 1 is therefore this statement's formalisation of a direction the source names, and two choices in it are ours rather than the source's. It asks for the plain Gilbert-Varshamov threshold, not for the *logarithmic improvement* on it that Gaborit and Zémor actually prove for double-circulant codes — the weaker target, chosen because it is what Theorem 1 needs and what the source appeals to. And it fixes the systematic form, for the reason in Remark 2. A

proof of the stronger statement with the logarithmic improvement, or a proof for some restricted family of abelian groups, is progress and should be reported as such.

Remark 2 (The caveat the source attaches, which is part of the statement). Without the systematic form the statement is false, and the source says why. A syndrome $s = a_1 e_1 + a_2 e_2$ lies in the ideal $(a_1, a_2) \subseteq \mathbb{F}_q[G]$ generated by the blocks of the parity-check matrix. Over a large field the blocks are invertible with overwhelming probability and that ideal is everything; over a small field it need not be, and then the syndrome distribution is biased — "when this ideal is not the full ring, there is an obvious bias".

In the growing-$|G|$ regime that is exactly the failure mode: "in the case of constant k, ℓ and growing $|G|$ there is a bias in the QA-SD distribution when the ideal generated by the blocks in the input parity-check matrix is not the full ring. This corresponds to the parity-check matrix not being full-rank when seen as a matrix over $\mathbb{F}_q[G]$. In this case, the minimum distance could drop, but heuristically a random quasi-G code will have a minimum distance linear in its length as long as this bias is removed, which is the case in our setting since we enforce the systematic form."

Note the word *heuristically*: this sentence is the source's reason for believing the conjecture, not an argument for it.

Remark 3 (Progress since, and what it leaves open). Li, Liu, Xing, Yao and Yuan give a fine-grained analysis of the minimum distance of random quasi-abelian codes of rank 1 and index c over $\mathbb{F}_q[(\mathbb{Z}/2\mathbb{Z})^n]$ for arbitrarily large prime fields, attaining the Gilbert-Varshamov bound up to an additive gap $n/(c \log_2 p)$; concretely, relative distance at least 0.4142 at rate $1/2$ over a 128-bit field with $|G| = 2^{20}$, against 0.1 for Spielman's code. They observe that their argument generalises to $\mathbb{F}_q[(\mathbb{Z}/d\mathbb{Z})^n]$ for $d \mid q-1$ and to a generic $\mathbb{F}_q[G]$ for a concrete group G.

That is real progress on Conjecture 1 and does not settle it, for a reason they state: their bound is non-asymptotic and becomes vacuous as $|G| \to \infty$. "While we can obtain a concretely high minimum distance from Theorem 1.1, it remains open whether QA code is asymptotically good for fixed index c and field size p, as our lower bound is meaningless when $|G| = N \to \infty$." They also restate the conjecture explicitly as the source's: "in [BCCD23] the authors

conjectured that Gaborit and Zémor's argument can be extended to arbitrary abelian groups and thus QA code approaches GV bound with $|G|$ going to infinity."

So the position on 28 August 2026: concrete bounds for particular groups over large fields, no asymptotic statement for growing $|G|$ beyond the cyclic case.

Remark 4 (Why it is worth settling). Conjecture 1 is what makes the choice of group free. The whole point of moving from quasi-cyclic to quasi-abelian codes is that groups such as $(\mathbb{Z}/3\mathbb{Z})^d$ give a ring in which sparse elements multiply to sparse elements and fast transforms exist, which is what lets pseudorandom correlation generators produce OLE correlations over small fields. Without the conjecture, resistance to linear tests is established only for the groups where a distance bound happens to be available.

The source is also explicit that the hardness of the underlying decoding problem is not in question in the same way: decoding a random quasi-abelian code "has been studied for over 50 years by the coding theory community and to this day, no efficient algorithm is known", and the problem is listed as open in the Encyclopedia of Coding Theory. What is missing is the distance bound, not the belief.

4 Bibliography

[BCCD23] Maxime Bombar, Geoffroy Couteau, Alain Couvreur and Clément Ducros. *Correlated pseudorandomness from the hardness of quasi-abelian decoding.* IACR ePrint 2023/845; CRYPTO 2023. The source. The conjecture is named on page 9 and again on page 20; quasi-G codes are defined in Section 4.1, the systematic-form caveat is Remark 18, the linear-test reduction is Section 4.5, and the Fan-Lin theorem is quoted there as Theorem 20.

[FL15] Yun Fan and Liren Lin. *Thresholds of random quasi-abelian codes.* IEEE Transactions on Information Theory, 61(1):82–90, 2015. The theorem in the fixed-group, growing-index regime, including the modular case; the statement the conjecture asks to transpose.

[GZ06] Philippe Gaborit and Gilles Zémor. *Asymptotic improvement of the Gilbert-Varshamov bound for linear codes.* Proc. IEEE International Symposium on Information Theory (ISIT) 2006, pages 287–291, Seattle, June 2006. The growing-group result for random double-circulant

codes, with a logarithmic improvement on the bound, whose extension to arbitrary abelian groups is the conjecture.

[Kas74] T. Kasami. *A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2.* IEEE Transactions on Information Theory, 20(5):679, 1974. The original Gilbert-Varshamov-like bound for quasi-cyclic codes that Gaborit and Zémor improve.

[Wil21] Wolfgang Willems. *Codes in group algebras*, chapter 16. Chapman and Hall/CRC, 2021. The Encyclopedia of Coding Theory chapter in which decoding random quasi-abelian codes is listed as an open research problem (Problem 16.10.5).

[LLXYY26] Zhe Li, Hongqing Liu, Chaoping Xing, Yizhou Yao and Chen Yuan. *More efficient SNARKs via quasi-abelian codes: faster, smaller, and field-agnostic.* IACR ePrint 2026/939. The progress described in Remark 3: concrete non-asymptotic minimum-distance bounds over $\mathbb{F}_q[(\mathbb{Z}/2\mathbb{Z})^n]$, and an explicit restatement of the source's conjecture as still open. [UNVERIFIED] — this is a follow-up found by literature search on 28 August 2026, not a citation read off the source's own reference list; the source predates it.

[Pie67] John N. Pierce. *Limit distribution of the minimum distance of random linear codes.* IEEE Transactions on Information Theory, 13(1):595–599, 1967. Cited by the source for the base case the conjecture generalises: random linear codes meet the Gilbert-Varshamov bound.