# GABRIEL PROTOCOL

{ ANOMAN DON, ARNAULT FRANÇOIS, NALDI SIMONE }

Université de Limoges

## SUMMARY

- **QUANTUM RANDOM NUMBER GENERATOR** based on violation of a free version of CHSH-3 expression, using Qutrits.
- Maximal quantum violation based security and Maximal entropy guaranteed under self-testing hypothesis

## ORIGINAL CHSH-3

**Requirement**

- 2 parties (A and B) and 2 measurements per party
- Measurements $A_i$ commute with $B_j$; their dimension is d=3

**Classical world inequality** [1, 2, 3]

$$\begin{aligned} I_3 = {} & P(A_1 = B_1) + P(A_2 = \omega^2 B_1) + P(A_2 = B_2) + P(A_1 = B_2) \\ & - P(A_1 = \omega^2 B_1) - P(A_2 = B_1) - P(A_2 = \omega^2 B_2) - P(A_1 = \omega B_2) \\ & \leq 2 \end{aligned} \tag{1}$$

**Specification**

- Not defined when observables $A_i$ do not commute with $B_j$
- Quantum upper bound [4]: $1 + \sqrt{11/3} \approx 2.9149$
- Algebraic upper bound : $4$

## FREE CHSH-3

**Requirement**

- 4 measurements with no constraints of parties
- Measurements do not necessarily commute; their dimension $d \geq 3$

**Classical world inequality**: decomposition of (1) using projectors

$$\begin{aligned} \langle \phi | & X_{1,1} X_{3,1} + X_{1,1} X_{4,1} - X_{1,1} X_{3,\omega} - X_{1,1} X_{4,\omega^2} + X_{1,\omega} X_{3,\omega} \\ & + X_{1,\omega} X_{4,\omega} - X_{1,\omega} X_{3,\omega^2} - X_{1,\omega} X_{4,1} + X_{1,\omega^2} X_{3,\omega^2} + X_{1,\omega^2} X_{4,\omega^2} \\ & - X_{1,\omega^2} X_{3,1} - X_{1,\omega^2} X_{4,\omega} + X_{2,1} X_{3,\omega} + X_{2,1} X_{4,1} - X_{2,1} X_{3,1} \\ & - X_{2,1} X_{4,\omega} + X_{2,\omega} X_{4,\omega} + X_{2,\omega} X_{3,\omega^2} - X_{2,\omega} X_{3,\omega} - X_{2,\omega} X_{4,\omega^2} \\ & + X_{2,\omega^2} X_{3,1} + X_{2,\omega^2} X_{4,\omega^2} - X_{2,\omega^2} X_{3,\omega^2} - X_{2,\omega^2} X_{4,1} | \phi \rangle \leq 2 \end{aligned} \tag{2}$$

**Specification**:

- Defined for non commuting observables.
- Quantum upper bound (using SDP) : $4$
- Algebraic upper bound : $24$

## OPTIMAL QUANTUM STATE AND MEASUREMENT FOR FREE CHSH-3

**Optimal state and projectors** obtained by SDP in the spirit of [5] :

4 operators of dimension $d = 3$ acting on **one party** prepared in the optimal state $|\phi^*\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$;

Projectors' vectors $|x_{1,1}\rangle, |x_{1,\omega}\rangle, |x_{1,\omega^2}\rangle, |x_{2,1}\rangle, \ldots, |x_{4,\omega^2}\rangle$ are given by the column of the matrix $\frac{\sqrt{3}}{9} \begin{bmatrix} 3 & 0 & 0 & 0 & 3 & 0 & 2 & -1 & 2 & 2 & 2 & -1 \\ 0 & 3 & 0 & 0 & 0 & 3 & 2 & 2 & -1 & -1 & 2 & 2 \\ 0 & 0 & 3 & 3 & 0 & 0 & -1 & 2 & 2 & 2 & -1 & 2 \end{bmatrix}$

**Observables:** $X_i^* = 1 \cdot |x_{i,1}\rangle\langle x_{i,1}| + \omega \cdot |x_{i,\omega}\rangle\langle x_{i,\omega}| + \omega^2 \cdot |x_{i,\omega^2}\rangle\langle x_{i,\omega^2}|$.

$$X_1^* = Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}; \quad X_2^* = \begin{bmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad X_3^* = \frac{1}{3} \begin{bmatrix} -\omega & 2 & 2\omega^2 \\ 2 & -\omega^2 & 2\omega \\ 2\omega^2 & 2\omega & -1 \end{bmatrix}; \quad X_4^* = \frac{1}{3} \begin{bmatrix} -\omega^2 & 2\omega & 2 \\ 2\omega & -1 & 2\omega^2 \\ 2 & 2\omega^2 & -\omega \end{bmatrix}$$

**Remark** : $X_1^*$ commute with $X_2^*$. The same for $X_3^*$ and $X_4^*$. **Measurement of $|\phi^*\rangle$ by $X_i^*$ gives $1$ or $\omega$ or $\omega^2$ with probability $1/3$**

## PROTOCOL EXECUTION

Repeat several times the next steps

**1)** Prepare a qutrit in the state $|\phi^*\rangle$. Select randomly a couple of measurement $(X_i^*, X_j^*)$; $i, j \in \{1, \ldots, 4\}$. (use public randomness source as that of the NIST)

**2)** If $i, j \in \{1, 2\}$ or $i, j \in \{3, 4\}$ (the chosen measurements commute) then measure the state $|\phi^*\rangle$ with $X_i^*$ and return the random trit $\omega^k, k \in 0, 1, 2$. **Measurement of $|\phi^*\rangle$ by $X_i^*$ gives $1$ or $\omega$ or $\omega^2$ with probability $1/3$ thus an min-entropy of 1 trit**

**2')** Else, measure the state $|\phi^*\rangle$ using $X_j^*$. Then collect the obtained state $|x_{j,\omega^k}\rangle$ and measure it using $X_i^*$. The obtained state is $|x_{i,\omega^\ell}\rangle$. Then return the tuple (" $|x_{j,\omega^k}\rangle$", "$|x_{i,\omega^\ell}\rangle$") for the evaluation of Bell quantity (2)

## SECURITY AND SELF TESTING ARGUMENTS

One evaluate Free CHSH-3 expectation using outcomes of step 2′. If this expectation is not equal to quantum bound $4$, the protocol is not valid.

In self-testing hypothesis, non malicious but error prone device, we guaranteed that, obtaining the maximal Bell value $4$ is equivalent to the fact of obtaining maximal min entropy

## REFERENCES

[1] D. Kaszlikowski, L. Kwek, J.-L. Chen, M. Żukowski, and C. Oh. Clauser-Horne inequality for three-state systems. *Phys. Rev. A*, 65:032118, Feb 2002.

[2] A. Acín, N. Durt, T. Gisin, and J. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65, 05 2002.

[3] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell Inequalities for Arbitrarily High-Dimensional Systems. *Phys. Rev. Lett.*, 88:040404, Jan 2002.

[4] L.-B. Fu, J.-L. Chen, and X.-G. Zhao. Maximal violation of Clauser-Horne-Shimony-Holt inequality for two qutrits. *Physical Review A*, 68, 09 2002.

[5] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM J. on Optimization*, 20(5):2157–2180,